COLETÂNEA DE ARTIGOS

EDIÇÃO IV - 2022

SUMARIO

SUMARIO

INTRODUÇÃO

Acelerado nos últimos anos, trazendo novas perspectivas às organizações. Apesar desta evolução, nos cabe fazer a seguinte pergunta: de que maneira o sistema de segurança gera vantagem competitiva.

Para construirmos esta resposta precisamos levar em conta três premissas. A primeira é que o sistema de segurança é uma unidade de apoio, unidade meio ou de serviço compartilhado, tal como recursos humanos, finanças e jurídico. Os produtos do sistema de segurança, assim como de outras unidades de apoio, são geralmente intangíveis, pois é uma prestação de serviço. É difícil quantificar esses produtos quando as empresas tentam avaliar a eficácia e a eficiência dessas unidades.

A segunda premissa é que o sistema de segurança precisa adotar um conjunto sistemático de processos a fim de criar valor por meio do alinhamento. Inicialmente, é necessário alinhar as estratégias do sistema de segurança com as estratégias das unidades de negócio e da corporação, definindo o conjunto de serviços estratégicos a serem oferecidos. Posteriormente, o sistema de segurança precisa alinhar seus processos, de maneira que sejam capazes de executar a estratégia. Para tanto, é necessário desenvolver um plano estratégico que descreva como adquirir, desenvolver e prestar serviço estratégico às unidades operacionais, o qual passa a ser a base do mapa estratégico, do Balanced Scorecard (BSC), da iniciativa estratégica e do orçamento do sistema de segurança. Finalmente, o sistema de segurança deve fechar o ciclo, avaliando o desempenho de sua iniciativa, mediante técnicas como acordo

de nível de serviço (SLA), feedback dos clientes internos, avaliações pelos clientes e auditorias internas.

A terceira premissa é perceber o sistema de segurança como um sistema aberto, ou seja, um conjunto de elementos dinamicamente relacionados que desenvolvem atividades para atingir determinado objetivo. Como sistema apresenta seis elementos: objetivos, entradas, processos, saídas e feedback.

O sistema de segurança cria vantagem competitiva se for excelente em qualquer dos arquétipos estratégicos adotados pelas unidades de negócio: baixo custo, liderança de serviço, soluções completas para os clientes internos. As estratégias de intimidade ou de soluções para os clientes exigem do sistema de segurança construir parcerias com os clientes internos, sendo necessário mudar de especialistas funcionais para assessores de confiança e parceiros do negócio.

O sistema de segurança reforça a estratégia empresarial por meio do portfólio de serviços que oferecem aos clientes internos. Depois de definir os serviços estratégicos, o sistema de segurança precisa desenvolver sua estratégia de prestação dos serviços prometidos, a qual, deve ser traduzida em mapa estratégico e em BSC. Ao se desenvolver o mapa estratégico e o BSC do sistema de segurança, é útil vê-lo como um negócio dentro de um negócio.

O BSC apresenta quatro perspectivas: financeira, cliente, processo interno e aprendizado e crescimento. A perspectiva financeira do BSC do sistema de segurança apresenta dois componentes: eficiência e eficácia. O primeiro envolve questões tradicionais, como o custo dos serviços prestados e a observância do orçamento. O segundo é medido pelo impacto sobre a estratégia empresarial.

Em relação à perspectiva dos clientes, devemos levar em conta que o sistema de segurança tem dois tipos de clientes:

- Os gestores das unidades de negócio a quem prestam serviços diretamente.
- Os colaboradores ou clientes externos, que são beneficiários e destinatários dos serviços.

O sistema de segurança deve compreender as estratégias dos clientes internos e usar sua expertise funcional para criar e propor soluções que contribuam para o sucesso desses clientes.

A perspectiva dos processos internos apresenta três temas. O primeiro é a concentração na excelência operacional que impulsionará o objetivo de eficiência da perspectiva financeira. O segundo tema trata da maneira como o sistema de segurança gerencia o relacionamento com os clientes internos. E o último tema aborda o apoio estratégico à

organização, impulsionando o componente de eficácia da estratégia, ao fornecer aos clientes internos novas capacidades que reforçam suas estratégias.

A perspectiva do aprendizado e crescimento trata das necessidades específicas dos recursos humanos do sistema de segurança, em termos de treinamento, tecnologia e clima de trabalho solidário. Em relação aos recursos humanos é necessário a preocupação com três componentes: programas de desenvolvimento de competências estratégicas; desenvolvimento da organização e da liderança; processo de gestão de desempenho.

Podemos perceber que se os objetivos do sistema de segurança forem desdobramentos dos objetivos de longo prazo desenvolvidos no planejamento estratégico da empresa, o sistema de segurança terá os seus processos relacionados com o negócio. Desta forma, o sistema de segurança terá a importância na obtenção do sucesso corporativo. Com esta potencialização, fez surgir a necessidade de departamentos de segurança com atuação científica, ou seja, não se admite mais o empirismo ou o "achismo" nas ações de segurança. Este contexto fez elevar o nível da prestação de serviços terceirizados de segurança ou de sistemas orgânicos de segurança. Para gerir o Sistema de Segurança é necessário um profissional altamente qualificado. Uma pessoa que gerencie de forma científica. Que saiba interagir a teoria com a prática. Alguém que tenha as competências (conhecimento, habilidade e comportamento) necessárias para ajudar a empresa a ser altamente competitiva. Esta necessidade criou a base para o surgimento dos cursos de graduação e pós-graduação na área de Segurança Empresarial. Cursos que são multidisciplinares e focados na prática. Mas para que os cursos cumpram com a sua missão é fundamental a existência de fontes de consulta. Baseado no exposto acima, é que estamos lançando mais uma edição da COLETÂNEA DE ARTIGOS. Uma coletânea de artigos que busca dotar os gestores dos conhecimentos necessários para serem capazes de fazer uma gestão científica e alinhada com a estratégia da empresa. Não queremos afirmar que os assuntos abordados nos diversos artigos estão esgotados, mas pontos importantes foram abordados. Além de abordarmos os pontos principais, temos o objetivo de despertar nos leitores a percepção da importância de aprofundamento dos diversos temas. São artigos produzidos por nossos sócios.

DESEJAMOS AOS LEITORES UMA ÓTIMA LEITURA E MUITO SUCESSO NA GESTÃO DOS SEUS DEPARTAMENTOS OU EMPRESAS.

EL TERRORISMO DOMESTICO: EVALUACIÓN DE RIESGO Y SEÑALES DE PELIGRO

Guillermo Alborno Mora
Delegado CEAS en Paraguay

La mayoría de las amenazas de los grupos antisociales resultan en un tipo de acción, por ello debemos prestarle atención y responder a todas las amenazas, ya sean escritas, verbales o físicas.

¿Qué tipos de amenazas deben preocuparnos?

- Cualquier amenaza o aviso de intención de amenaza de bomba, asesinatos y crímenes selectivos de autoridades, etc.
- Cualquier amenaza de hacer algo peligroso o potencialmente destructivo.
- La posesión o el acceso a armas automáticas.

Cuando un grupo antisocial hace una amenaza, debemos considerar lo siguiente:

- ¿Con cuánta seriedad se hizo la amenaza?
- ¿Qué otra información tenemos sobre el grupo antisocial que hizo la amenaza?
- ¿Tiene el grupo antisocial un plan para llevar a cabo la amenaza?
- ¿Tiene el grupo antisocial los medios para llevar a cabo la amenaza?

Para ayudarnos a evaluar las primeras dos preguntas, debemos tomar en cuenta las señales de peligro o “banderas rojas” que según los investigadores están más asociadas con la violencia delincuencial:

- Historial de comportamiento violento o agresivo
- Patrón de amenazar con violencia
- Historial de destrucción de propiedad o comportamiento criminal
- Historial de crueldad hacia las sociedades urbanas.
- Historial de comenzar incendios
- Historial de conflictos o problemas intercomunitarios
- Relación con pandillas urbanas y capas de narcotraficantes

Debemos evaluar cualquier amenaza dentro del contexto del comportamiento pasado del grupo antisocial, la personalidad de sus miembros y los factores de motivación que puedan tener en el momento de la amenaza.

Para ayudar en la evaluación, debemos considerar si la amenaza o el plan es realista o si puede llevarse a cabo; por ejemplo, un delincuente común que amenace con tirarle una bomba a la comitiva del Presidente de la República probablemente presente un riesgo menor que un guerrillero que amenace con pegarle un tiro a una autoridad política del país y matarlo.

Si el grupo antisocial tiene acceso a pistolas u otras armas, la amenaza se eleva a un nivel potencialmente mortal. Para evaluar el riesgo de violencia, será importante determinar si hay armas en el grupo delictivo o si el grupo antisocial participa en una pandilla que pueda tener acceso a armas.

CONFLICTO, VIOLENCIA Y PROTESTA SOCIAL

Guillermo Alborno Mora
Delegado CEAS en Paraguay

El conflicto es una construcción conceptual abstracta, no perceptible por nuestros sentidos. No así la violencia. En la presente nos adentraremos en el estudio de la misma.

Al tratarse de una conducta, podemos afirmar a priori que:

Violencia = Violencia Directa + Violencia Estructural + Violencia Ideológica

La violencia estructural es aquella que se origina en la injusticia y/o en la desigualdad / inequidad de la propia estructura social o entre diversas sociedades.

La violencia ideológica es la que a través de la manipulación e influencia de determinadas ideas y acciones sobre una sociedad o "grupo blanco", trata de legitimar la violencia estructural.

Es utilizada hábilmente por personajes influyentes a través de los medios de comunicación masiva, con el objeto de adquirir y acrecentar cuotas de poder en el ámbito político, transculturizar o dominar, con fines que no se expresan.

La violencia directa es un acontecimiento físico, normalmente sangriento. La violencia estructural es un proceso o una situación, con altos y bajos y la violencia ideológica es una agresión indirecta, casi invariable y sutil a lo largo del tiempo, dado el ritmo dosificado y de lenta transformación que normalmente exige el objetivo que se persigue.

Crear y consolidar un estadio de manejo de conflicto, como fin último de cualquier Política de Seguridad Pública Interior, exige prever y evitar la violencia antes que aparezca o reduciéndola, en el caso de que se manifieste. Ello requiere la consideración de los tres tipos de violencia al mismo tiempo, en el planeamiento. Superar a una de las tres, no conduce automáticamente a eliminar a las otras dos.

La violencia ideológica, la violencia estructural y la violencia directa, no pueden solucionarse solo con más violencia.

Ello llevaría a nuevas formas violentas y además escalaría a una espiral incontenible.

La forma de romper este círculo vicioso es recuperar la estructura institucional y hacer operativos a los mecanismos adecuados para resolver los conflictos sociales, por medios no violentos.

Ese mecanismo es el Sistema Político de manejo de conflictos sociales no resueltos., con ello tendremos un correcto funcionamiento de la administración de las crisis producto de los conflictos de clases no resueltos, para desterrar la violencia y el uso de la violencia.

Nos impresiona el descontrol de la violencia directa y la escalada de hechos violentos sin ningún tipo de previsión ni control.

La violencia estructural es cada vez más acentuada y profunda. Los niveles de pobreza de grandes sectores sociales, la marginalidad creciente, la constante desindustrialización, la problemática de los sectores rurales, la falta de acceso a la formación espiritual de nuestros jóvenes, los crecientes índices de mortalidad y desnutrición infantil, el narcotráfico como único recurso de subsistencia de grandes sectores sociales, conforman un cuadro crítico y explosivo.

Pero es la violencia ideológica la más sutil y la más perniciosa de todas, dado que es la explota a las anteriores y la que está más estrechamente vinculada con el Sistema Político, del cual precisamente debemos esperar las soluciones.

¿Cuántas veces hemos escuchado a encumbrados representantes del sistema político justificar la violencia directa con los argumentos de la violencia estructural, instrumentando un contenido netamente ideológico? Este es el camino que hemos venido transitando y el resultado está a la vista: la sociedad anarquizada, la Instituciones vaciadas de contenido y el Estado desmembrado.

Solamente podremos contener a la violencia generalizada que hoy nos aplasta cuando nuestros líderes encuentren el camino de la Política de Estado, que es la visión arquitectónica del País que queremos, asentada en nuestra realidad y cuyo valor central es la afirmación cultural de la Nación.

Ello nos permitirá abarcar y resolver nuestros sangrientos conflictos, alentados hasta hoy por los ideólogos transculturizados. Los “revolucionarios” que hacen simplemente ideología y que se han infiltrado en el sistema.

Eso es lo que está fatigando la paciencia de un pueblo que hoy “sobrevive” o “subsiste”, con graves dificultades y sin rumbo. Por ello queremos terminar INSISTIENDO EN LA NECESIDAD DE QUE LA AUTORIDAD POLITICA Y LA POLICIA encuentren alternativas de manejo de los conflictos sociales, bajo el conocimiento que las PROTESTAS EXIGEN RESPUESTAS.

IMPLANTAÇÃO DA NORMA INTERNACIONAL "ISO 28000: SISTEMAS DE GESTÃO DA SEGURANÇA PARA A CADEIA DE SUPRIMENTO"

Manuel Sánchez Gómez-Merelo

Consultor Internacional de Seguridad Pública y Privada
Presidente · Director General de GET (Grupo Estudios Técnicos)
Director de Programas de Seguridad del Instituto Universitario
General Gutiérrez Mellado IUGM-UNED

Recordemos… O que é uma norma? As normas são um modelo, um padrão, exemplo ou um critério a seguir. Uma norma é uma fórmula que tem valor de regra e tem por finalidade definir as características que deve ter um objeto ou método compatível para ser usados a nível internacional.

A ISO (International Standaritation Organization) é a entidade internacional encarregada de favorecer a normalização no mundo, com sede em Genebra, é uma federação de Organismos.

A finalidade principal das normas ISO é orientar, coordenar, simplificar e unificar os usos para conseguir menores custos e maior eficiência e eficácia.

OS ANTECEDENTES DA ISO 28000

Como consequência da incerteza mundial criada com os atentados de 11 de setembro de 2001 nos EUA as entidades públicas e empresas privadas começaram a ter maior conscientização da necessidade de proteção de seus bens e ativos.

Neste sentido, além da legislação de obrigado cumprimento, uma série de normas internacionais foram vendo a luz, normatiza nas que se contêm requisitos específicos para garantir a proteção de cada um dos processos das empresas e as infraestruturas críticas mais significativas.

O desenvolvimento e a promulgação de um marco legislativo novo, assim como de políticas específicas para a proteção de infraestruturas críticas foi um avanço dentro do âmbito da segurança.

dentro de pouco tempo, a norma UNE-ISO 28000, será imprescindível em instalações portuárias, aeroportos, grandes centros comerciais, companhias de fornecimento de energia, empresas de transporte e setor ferroviário, entre as principais.

A NORMA ISO 28000 E SEUS OBJETIVOS

A Norma Internacional "ISO 28000: Especificações para os sistemas de gestão da segurança para a cadeia de suprimento", foi criada como um padrão internacional válido que combina as diferentes necessidades existentes destas empresas e instalações com uma série de requisitos e análise a levar a cabo para conhecer os pontos de controle críticos e atuar contra os possíveis riscos, ameaças e vulnerabilidades.

A norma ISO 28000 especifica os requisitos necessários para garantir o sistema de gestão da segurança, destacando aqueles aspectos críticos para o desenvolvimento e a proteção da atividade.

Esta norma, ainda de escassa implantação, define as especificações para os sistemas de organização e gestão da segurança para todas as fases da cadeia de suprimento.

A implantação desta norma e o incremento do nível de segurança neste entorno, sobre a base dos riscos identificados, analisados e avaliados para cada organização, requererá levar a cabo uma série de medidas corretivas concretas, eficazes e econômicas para manter a continuidade da atividade em caso de crise.

Neste sentido, a alta Direção deve assegurar a continuidade da atividade ou negócio e garantir ao máximo a proteção das pessoas e bens. Para isso é necessária uma implicação direta e avaliar qualquer oportunidade de melhora para evitar riscos que possam pôr em situação crítica a organização ou atividade.

Do ponto de vista metodológico, a norma segue o típico ciclo PDCA ((Plan, do, check, action). Entretanto cabe destacar que o enfoque utilizado já não é o apoiado em processos do sistema de gestão (ao estilo da ISO 9001:2000), mas sim, como vem acontecendo com outras normas dos últimos anos, como a ISO 27000, trata-se de um enfoque apoiado na identificação e avaliação do risco. Todo isso alinhado com a política de segurança da organização e assegurando que as medidas adotadas sejam coerentes com a magnitude de suas atividades ou operações.

O ÂMBITO DE APLICAÇÃO E SUAS VANTAGENS

Como se indicou, esta norma internacional ISO 28000, pode aplicar-se em organizações de qualquer tamanho, da fabricação ao serviço, passando pelo armazenamento ou o transporte por mar, estrada, via aérea ou ferrovia e em qualquer das fases de produção ou fornecimento.

Certificando este sistema de gestão de segurança, a organização conhecerá perfeitamente seus processos críticos, estratégicos e operativos ou táticos, para o desenvolvimento das atividades industriais ou comerciais e terá a capacidade de determinar que operações preventivas se realizam ou devem levar-se a cabo, com que meios e recursos contam e devem contar, e em que prazos se devem executar.

Em resumo, a chave reside na identificação, análise e avaliação dos riscos que permite saber à organização ou atividade:

- A situação real em que se encontra quanto a seus riscos e sua proteção.
- As vulnerabilidades, riscos e ameaças existentes.
- O impacto do potencial materialização destes riscos ou ameaças.
- Os riscos concretos assumidos.
- A dimensão das medidas de controle e segurança a implementar para a diminuição ou controle do impacto ou consequências.

Desta avaliação se obterá a informação necessária para:

- Estabelecer os objetivos para a gestão da segurança.
- Definir os requisitos para o desenho, a especificação e a implantação.
- Estabelecer os programas de gestão da segurança.
- Identificar e dimensionar os recursos necessários.
- Determinar e desenvolver os controles operacionais.
- Identificar as necessidades de formação e capacitação.

O plano de segurança deverá estar perfeitamente documentado, e incluir os procedimentos necessários e adequados. Dito plano deverá ser comunicado a todos e cada um os implicados segundo suas responsabilidades tendo em conta a confidencialidade que leva implícita a informação relacionada com a segurança e sua gestão.

Neste sentido, as principais vantagens da certificação no ISO 28000 são:

- Garantir que se levam a cabo operações para o controle dos riscos e a implantação de medidas que as podem diminuir.
- Certificar por uma terceira parte, que o sistema de gestão da segurança da cadeia de fornecimento da organização se leva sob os padrões internacionais estabelecidos na norma ISO 28000.
- Poder comunicar a clientes ou usuários, autoridades e investidores a implantação do sistema de gestão da segurança e utilizá-lo como ferramenta competitiva e diferencial.
- Contribuir um valor acrescentado e diferencial para a organização nas operações ou atividades industriais ou comerciais.

Em resumo, uma nova norma que, conforme se vá generalizando sua implantação, terá como consequência a especial melhora da segurança na cadeia de fornecimento global e no das infraestruturas críticas, em particular.

ELEMENTOS DO SISTEMA DE GESTÃO DA SEGURANÇA COM A ISO 28000

Os elementos básicos e fundamentais a ter em conta para o correto desenvolvimento e implantação da norma são entre outros:

- Requisitos gerais
- Política de segurança
- Identificação e Avaliação dos riscos
- Implementação da norma
- Auditoria e ações corretivas
- A modo de conclusões

Embora, na teoria, esta norma internacional é aplicável a organizações de qualquer tamanho que trabalhem em todas e cada uma das fases da cadeia de fornecimento, na prática parece ter sido pensada, especial e fundamentalmente, para a gestão da segurança relacionada com o transporte marítimo.

Em qualquer caso, através da implantação e certificação ISO 28000 se evitarão danos a pessoas, bens e meio ambiente, a mesma abrange áreas como o transporte de matérias perigosas e instalações desenhadas para as receber, proteção da cadeia em infraestruturas críticas, controle dos processos de alfândegas, etc.

Entre os principais benefícios da implementação da norma, poderiam destacar-se alguns como: a redução dos riscos, ao verificar que empresas e entidades cumprem com os requerimentos internacionais de segurança da cadeia de fornecimento; a melhora e seguro da qualidade e o controle do produtor; a integração das normas existentes de segurança relacionada, principalmente com o transporte, em um sistema de gestão unificado; o facilitar as importações e a gestão de documentação nas alfândegas; e a implantação de metodologia na gestão e rastreabilidade das infraestruturas críticas.

Sem dúvida, a implantação da ISO 2800 cria e criará um especial avanço em matéria de integração e globalização da segurança.

A NOVA GESTÃO EM SEGURANÇA CORPORATIVA

Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad Pública y Privada
Presidente · Director General de GET (Grupo Estudios Técnicos)
Director de Programas de Seguridad del Instituto Universitario
General Gutiérrez Mellado IUGM-UNED

Desde o início deste século, o mundo foi fortemente abalado e alguns paradigmas foram quebrados, pelo menos três vezes, por: os atentados de 11 de setembro de 2001, o colapso financeiro de 2008 e, muito especialmente, pela pandemia de COVID-19, ainda em curso.

Cada caso foi uma ameaça assimétrica, desencadeada por algo aparentemente específico e muito diferente de tudo o que o mundo experimentou até então.

Só precisamos ver como foi 2020 para ter uma ideia de quão dinâmico e imprevisível o mundo é hoje. Lenin disse: “Há décadas em que nada acontece e semanas em que décadas passam.”

Como já dissemos, neste ano irrepetível de 2020, para além da extraordinária solidariedade e resiliência demonstrada pela população em geral e por alguns grupos profissionais em particular, três palavras parecem ter protagonizado tudo o que aconteceu: incerteza, insegurança e pessimismo.

A insegurança tem revelado uma lista incontável de vulnerabilidades em todo o mundo em todos os tipos de setores, especialmente na saúde, turismo, serviços, transporte, comércio, etc.

Esta situação inusitada nos predispôs a reconsiderar a importância de rever valores e tentar nos reinventar em algo tão básico como a liderança e a gestão em todos

os níveis (político, institucional, empresarial e pessoal), enfrentando desafios e oportunidades com todas as garantias.

As consequências políticas, sociais, tecnológicas e econômicas podem levar anos para desaparecer e, enquanto isso, vivemos um ressurgimento da vida digital ou virtual, um presente e futuro diferentes diante da globalização e uma nova ordem mundial emergente, dividida entre a China e os Estados Unidos. Em qualquer caso, o futuro permanece verdadeiramente em nossas mãos.

Estamos diante de um novo aprimoramento que podemos resumir na sigla apresentada anteriormente de **L.I.D.E.R.A.R.** com confiança, a fim de abordar prontamente sete elementos essenciais, tais como:

- **Linhas mestras**, para alcançar de forma coordenada e sustentável o novo normal que a sociedade em geral e as suas atividades em particular exigem.
- **Inovação**, para dar uma resposta eficiente e duradoura aos novos desafios e oportunidades que a crise (principalmente a crise da saúde) emergiu.
- **Decisão**, com base na experiência e no conhecimento, implementando o mais rapidamente possível as novas estruturas e protocolos que permitem atuar com a máxima segurança e garantias.
- **Ética**, aplicar com rigor e equilíbrio tudo o que precede, e responder à sociedade com medidas solidárias e soluções sustentáveis, de acordo com as novas situações criadas.
- **Responsabilidade**, como base de trabalho em todas as áreas institucionais, empresariais, pessoais e sociais.
- **Autenticidade**, transparência e rigor em todos os tipos de decisões, ações e novas abordagens de acordo com a nova ordem mundial.
- O **respeito** prioritário à solidariedade e à segurança humana, como um direito global de todos os povos, para enfrentar de forma global e eficiente todos os desafios e novas demandas deste novo futuro.

GESTÃO DE RISCO E SEGURANÇA

A segurança é o eixo do novo normal e tornou-se um fator indispensável e incontornável em todas as áreas durante a crise de saúde que vivemos.

Nos últimos tempos, novos riscos e demandas surgiram derivados da situação gerada pela pandemia, tanto no nível da segurança global como da segurança humana e

privada, desde o mundo que compartilhamos até a dimensão pessoal (mundo, país, cidade, bairro, casa, pessoa).

A Nova Gestão Corporativa e Segurança, de Manuel Sánchez Gómez-Merelo Nesse sentido, a Gestão de Riscos e Segurança é essencial em todos os ambientes e, especialmente, no campo do trabalho e no desenvolvimento das organizações institucionais e empresariais, onde o tema é complexo e multidisciplinar.

É necessária uma gestão coordenada e preventiva dos riscos e ameaças: uma visão multidisciplinar e profissional de segurança (prevenção + proteção), bem como um alinhamento dos riscos ao nível da organização (reputação e ética, posicionamento no setor, informação, recursos humanos, conformidade legal, continuidade, contingência e resiliência).

A identificação, classificação, análise e avaliação dos riscos e conhecimento das vulnerabilidades são peças fundamentais para o estabelecimento de um Plano Diretor de Segurança, uma vez que a partir da avaliação final dos mesmos, determinados sistemas e subsistemas de segurança serão articulados e implementados. (Prevenção + proteção) básico e suporte, bem como os protocolos de gerenciamento correspondentes.

Ao avaliar o resultado da análise de risco, devemos levar em consideração a disponibilidade de recursos humanos, materiais e financeiros que a organização possui.

Com tudo isso, será elaborado um documento único e integrador no qual se reflete o sistema de Gestão de Riscos e Segurança da organização.

Os objetivos fundamentais do plano são: minimizar e, na melhor das hipóteses, neutralizar os riscos e ameaças detectados e reduzir ao máximo as consequências negativas da sua concretização e impacto.

GESTÃO DE RISCOS E MONITORAMENTO DE SEGURANÇA

Com base numa nova visão holística de Gestão de Riscos e Segurança, propomos o desenvolvimento de uma nova aplicação, integrada por conceitos de inovação especial e aspectos diferenciadores no domínio dos riscos, ameaças e vulnerabilidades, principalmente para ambientes corporativos.

A Nova Direção Corporativa e Segurança, de Manuel Sánchez Gómez-Merelo Para o desenvolvimento do plano de Gestão de Risco e Segurança podemos basear-nos em diferentes normas como a Norma ISO / IEC 31.000, com possibilidades de utilização e adaptação a qualquer organização, bem como experiências em segurança em ambientes corporativos e institucionais.

Esta aplicação abrangente e nova metodologia de Gestão de Riscos e Segurança é uma nova visão que faz referência especial à mudança do paradigma de segurança em entidades empresariais com metodologia e gestão sistemáticas.

Adicionalmente, incluirá desenvolvimentos específicos para análise de risco de novos negócios e unidades de atividade e avaliação de novos projetos da entidade na perspectiva de riscos e segurança (investimento no estrangeiro, projetos de desenvolvimento, aquisições, etc.).

O desenvolvimento do seu conteúdo exigirá: a identificação, classificação, análise e avaliação rigorosa de todos os riscos e ameaças da organização; a identificação e descrição das vulnerabilidades e suas atividades; a abordagem de gerenciamento de risco abrangente; a análise de probabilidade e impacto; e o estabelecimento de um plano abrangente para o tratamento dos riscos, ameaças e vulnerabilidades identificadas.

A nova abordagem de gestão e segurança corporativa é necessária para ressegurar: Atividades (industrial, comercial, social); Transporte (internacional, nacional, local); Economia (global, local); Educação e treinamento (nacional, local, pessoal); Segurança (prevenção, proteção); Trabalho (negócios, autônomo); Saúde (global, local, pessoal) e um longo etc.

NOVA NORMALIDADE. LIDERAR A TRANSFORMAÇÃO DIGITAL COM SEGURANÇA

Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad Pública y Privada
Presidente · Director General de GET (Grupo Estudios Técnicos)
Director de Programas de Seguridad del Instituto Universitario
General Gutiérrez Mellado IUGM-UNED

A aceleração da transformação digital é possivelmente, o projeto a nível global mais importante e urgente como consequência do vivido e as mudanças que estamos tendo durante o largo processo desta pandemia provocada pela COVID-19 desde finais do ano 2019.

Umas mudanças que, em diversos aspectos está e vai supor uma verdadeira mutação de paradigmas, como o é no caso da digitalização de todos os setores e atividades, independentemente do nível ou dimensão das instituições e organizações.

Uma mudança de paradigmas, como o é no caso da segurança que afeta ao global e o glocal de forma transversal a todos os setores e atividades industriais e comerciais e às Administrações Públicas e, de maneira muito especial, às infraestruturas essenciais, estratégicas e críticas.

Glocal é o intercâmbio entre valores culturais globais e locais, gerando um terceiro valor, que enfatiza, simultaneamente, os dois primeiros.

Por tudo isso, e como já vamos insistindo faz tempo que, a segurança é e será o conceito transversal protagonista em todo este processo de digitalização e transformação digital.

Uma transformação digital, liderada por uma Segurança integral, operativa e tecnológica, pública e privada, física e lógica com o objetivo de reforçar os controles, capitalizar a analítica de dados, colaborar mais com todos os membros da organização,

dinamizar a resposta e aumentar a resiliência e atacar as prioridades, as novas provocações, exigências e oportunidades que se apresentam nas entidades públicas e privadas nesta fase da recuperação e para a nova normalidade depois da pandemia.

A segurança liderará esta recuperação com todos os meios a nosso alcance onde, as organizações, têm que implementar a prática de influir ou convencer, e pensar-lhe muito antes de impor novos médios e medidas de segurança, sem a análise prévia em profundidade e de forma integral, a fim de evitar batalhas internas na hora de aplicar os sempre limitados recursos ali onde sejam mais benéficos para a redução de ameaças e a eficiente gestão do risco e as seguranças.

Uma transformação digital, digitalização e automatização, onde seus aspectos mais importantes dentro da segurança são a prevenção e a resiliência, como crava para a nova normalidade.

Uma nova colocação de segurança integral e integrada apoiada nas lições aprendidas durante esta pandemia que requer reavaliação e implementação de uma: Análise das novas necessidades e exigências do mercado; Avaliação da situação atual das seguranças depois da pandemia; Visão estratégica, global e coordenada; Colocação da Gestão integral do Risco e as Seguranças; Estudo dos novos produtos e serviços, segundo exigências e necessidades; Capacitação especializada para os novos objetivos, implementações e serviços; Novos protocolos para a Cooperação Público-privada; Revisão e adequação das carências de Legislação e Normativa; Revisão das novas provocações para o setor das seguranças (física e lógica), especialmente em matéria de cibersegurança; Avaliação das novas oportunidades.

Estamos ante uma mudança de modelo de segurança global e glocal. O mundo trocou por completo depois de uma pandemia que acelerou o processo de transformação digital, e agora é chave para as organizações dispor de uns recursos humanos e técnicos que estejam preparados e protegidos em sua gestão desde qualquer lugar e dispositivo.

Igualmente, durante a pandemia, o teletrabalho em certo tipo de funções e tarefas veio para ficar em nosso modelo empresarial e institucional, insistindo às organizações a acelerar seu processo de transformação digital e ao uso das novas tecnologias para procurar relações de trabalho seguras de e com seus empregados, com as exceções a nível de medidas impostas, assinaladas na normativa vigente, e que serão objeto imprescindível de atualização obrigatória já no presente e nos próximos tempos.

A modo de resumo, como já viemos dizendo e, tendo em conta que a segurança é um conceito vivo e dinâmico, nos últimos tempos, e especialmente em ano passado, os pilares sobre os que se assentava este conceito transversal de segurança (prevenção + proteção), deterioraram-se e cambaleado, em grande medida em relação com aspectos também relacionados com a própria globalização. Entretanto, as bases esquemáticas da segurança são suficientemente fortes para confrontar o que vier,

em meio desta nova singradura através das ameaçadoras enjoa ou ondas de uma pandemia onde tudo foi e é novo.

Já, a União Europeia, em sua primeira publicação da Estratégia de Segurança no ano 2003, assinalava a necessidade de confrontar juntos as ameaças e riscos existentes, recordando, por outra parte, que nenhum país por si mesmo seria capaz de fazê-lo a sós.

Assim, temos que avançar baixo as bases de uma governança global os desafios e a mudança existente no planeta para um mundo mais seguro com as responsabilidades compartilhadas, com essas ameaças à paz e a segurança, entre as quais as referências às enfermidades infecciosas mortais são constantes, assim como à necessidade de uma segurança biológica que também põe de manifesto as vulnerabilidades de nossos sistemas sanitários -a escala global- frente às novas enfermidades infecciosas, abundando nos riscos (e oportunidades) que geram os avanços na biotecnologia, o que faz necessário preparar uma defesa eficaz contra o bioterrorismo e contra os brotos naturais de enfermidades infecciosas.

Finalmente, ante este novo modelo de segurança global, de grande amplitude e complexidade, não podemos perder de vista todas essas palavras/conceptos chave com os que temos que seguir trabalhando que são principalmente a: Globalização, Glocalizacão, Revisão, Atualização, Transformação, Digitalização, Reinvenção, Prevenção, Integração, Convergência, Controle, Cibersegurança, Tecnologia, Gestão Integral, Resiliência, Cooperação, Capacitação, Eficiência, Produtividade… todo isso, imprescindível para a "Nova normalidade", com a transformação digital liderada pela segurança.

Glocalização é um neologismo resultante da fusão dos termos global e local. Refere-se à presença da dimensão local na produção de uma cultura global.

O CÍRCULO ESTRATÉGICO E AS COMPETÊNCIAS ESSENCIAIS

Jefferson W. Santos Cel Av R1 MSc

Coronel Aviador da Aeronáutica (Reserva); bacharel em Ciências Aeronáuticas e Administração de Empresas, possui MBA em Gestão Estratégica de Pessoas pela FGV Brasília, Pós-graduação em Segurança e Defesa Hemisféricas pelo Interamerican Defense College (Washington – USA), Mestrado em Ciências Aeroespaciais na Universidade da Força Aérea (Rio de Janeiro- RJ) e Mestrado em Segurança e Defesa Hemisféricas pela Universidad del Salvador e Interamerican Defense College. Piloto Civil pela ANAC (Agência Nacional de Aviação Civil – Cód 138 480).

Qualquer atividade, em qualquer setor, que uma empresa ou uma organização execute, visa atender às necessidades, demandas ou vontades de um cliente.

Seja um cliente interno ou externo (nestes inclusos órgãos públicos e agências reguladoras), essa demanda se traduz em uma entrega. Portanto, um bem ou um serviço (seja uma camisa, um tênis, um carro, uma consultoria, um protocolo, uma certificação, um atendimento médico, jurídico, psicológico, cartorial etc.). Todos seguem um **CÍRCULO BÁSICO**: Um início, um processamento, uma entrega e um feedback.

O INÍCIO DO CÍRCULO

O cliente como início desse círculo apresenta uma vontade (ou uma expectativa de entrega), que precisa ser verificada se é viável, factível ou legal.

Pode ou não ser feito?

Ato contínuo, a empresa verifica suas competências, recursos, métodos e o tempo disponível antes de se prosseguir com as buscas e aquisições de insumos, chegada destes ao centro de processamento, transformação do insumo em um produto (bem ou serviço) e entrega como o cliente apresentou como requisitos e expectativas.

OS AMBIENTES EXTERNO E INTERNO PERMITEM FAZER?

Como vivemos em uma realidade econômica onde a figura do Estado é muito presente e incidente na atividade produtiva, este **CÍRCULO** sofre interferências do ambiente externo, seja por intermédio de ações dos agentes intervenientes (públicos ou privados) ou deficiências na infraestrutura crítica ou humana. Em função dessa realidade, as lideranças na empresa precisam se certificar o nível de dificuldades ou de desafios com os quais os elementos externos irão dificultar a produtividade e a eficiência da entrega do produto nas condições demandadas pelo cliente.

A ENTREGA E O FEEDBACK

Uma vez que o bem ou o serviço é entregue, o ecossistema produtivo aguarda o feedback do cliente para consolidar as metodologias e recursos usados na produção ou corrigir até a satisfação plena do cliente.

Sempre em busca de excelência e de competividade, as lideranças registram todos os atos, processos, sistemas e metodologias para, em produtos futuros, apresentarem os mesmos níveis de excelência ou aperfeiçoá-los em função das evoluções do mercado.

O principal ator desse ecossistema produtivo é o funcionário. Sendo executivo ou líder de equipes, há um pressuposto ético básico de que, uma vez contratado, ele irá desempenhar suas competências e habilidades conforme asseverou nas fases de recrutamento e de seleção estruturada pela empresa em busca de mão de obra qualificada e preparada para os desafios aos quais ela tem expectativa que a contratação vá atender.

Você, como partícipe operativo e operacional desse círculo irá apresentar e aplicar as competências essenciais para, fazendo parte de uma grande? Sinfonia? entregar suas competências.

Quais seriam, em meu entender, tais competências essenciais?

Ressalto que essa seleção adveio de aprendizado imersos em consistentes desafios junto a um variado, mas valoroso, elenco de colaboradores em mais de dez organizações distintas, ao longo de mais de 30 anos. Segue o elenco:

O conhecimento:

- Não só em termos de expertise específica para a elaboração do produto (bem ou serviço) requerido pelo cliente,

A Consciência Situacional (Situation Awareness):

- Refere-se às condições e óbices existentes tanto nos ambientes externos como interno da empresa;
- Considera a capacidade de se ver e de se entender como os elementos da infraestrutura crítica e a humana, além dos órgãos públicos e agências reguladoras interferem na eficiência e na produtividade dos indivíduos e dos setores da empresa;

A comunicação:

- Como competência essencial para se traduzir e disseminar o que você conhece, em termos de orientações ou de diretrizes;
- Refere-se à capacidade de se traduzir, para entendimento simples, todos os eventos, fatores e fenômenos que você percebe que venham tanto auxiliar como prejudicar a eficiência e a produtividade do setor onde você trabalha bem como os setores adjacentes;

A articulação:

- É a capacidade de se verificar antecipadamente as condições que os colaboradores e setores envolvidos terão antes de se iniciar os processos de elaboração do produto (bem ou serviço) demandado pelo cliente;
- Também pressupõe a capacidade de buscar os meios, os recursos e os métodos necessários para compensar eventuais deficiências, permitindo que funcionários e setores deem o melhor de suas competências para aderirem à elaboração do produto requerido;

A coordenação:

- É uma competência essencial para qualquer tipo de atividade conjunta ou colaborativa. A fase da coordenação que, necessariamente, deve vir após a fase da articulação as atividades, sejam administrativas ou operacionais e devem apresentar uma sequência lógica de execução. As demandas e resultados de cada atividade em cada setor são interdependentes assim, é uma competência fundamental para uma liderança eficiente;

O controle:

- É fundamental para que eventuais erros ou resultados fora do gabarito ou dos parâmetros estabelecidos tenham sua correção executada de forma oportuna e sem demoras; e

O feedback:

- É uma competência essencial para o encerramento do CÍRCULO;
- Ela permite com que todos os integrantes do ecossistema produtivo tenham condições de avaliar a propriedade de suas formas de produção bem como conhecer, de forma clara e consistente, eventuais erros que carecem de correção e a forma com as correções devam ser aplicadas.

Nos anos que passei frente a mais de 400 colaboradores distintos, em mais de dez organizações diferentes, espalhadas em mais de seis estados do território, percebi ao longo das atividades de instrução, de orientação funcional ou de mentoria que o entendimento do CÍRCULO ESTRATÉGICO e das COMPETÊNCIAS ESSENCIAIS era o que tornava o desempenho individual e setorial eficiente, com elevados níveis e produtividade e, portanto, competitivo.

Vale a pena tentar. Boa sorte e sucesso.

Visite a Página ADASTRA. Convido a assinar a newsletter. Sempre estou postando material de qualidade para auxiliar na gestão estratégica das empresas.

CONTATOS

Jefferson Wanderley dos Santos MSc
ANAC 138.480
081 97111 0211 Vivo
081 3033 6593 (r) Vivo
@adastrapilot
www.adastrapilot.com

O DESAFIO DE SALVAGUARDAR INFRAESTRUTURAS CRÍTICAS DE ENERGIA ELÉTRICA EM ÁREAS URBANAS

Anderson Moura, MBS, CPSI, CIGR, CIEIE, EAR, MBA
Gestor de Segurança Especialista no Setor Elétrico

Há muito tempo, a ausência de energia elétrica afeta diretamente a vida das pessoas, inclusive, trata-se de fator de risco a nível de Estado. Em virtude disso as geradoras, transmissoras e distribuidoras de energia elétrica possuem a árdua missão de salvaguardar suas infraestruturas críticas de energia elétrica.

A energia elétrica do Brasil é gerada por quase 5 mil usinas que utilizam diversas fontes de geração, como água, vento, sol, biomassa, combustíveis fósseis e a energia térmica liberada em reações nucleares.

A Agência Nacional de Energia Elétrica (ANEEL) aponta que o Brasil possui 105 distribuidoras de energia elétrica, sendo 54 concessionárias e 38 permissionárias, além de 13 cooperativas de eletrização rural.

O fornecimento de energia elétrica ao consumidor final é realizado através de infraestruturas físicas distribuídas em ativos de grande dimensão e complexidade, dispostos em áreas de possível vulnerabilidade, onde eventos criminosos podem interferir diretamente ou indiretamente no funcionamento do sistema, tendo graves consequências à população.

Pode-se afirmar que os crimes contra o patrimônio são os principais riscos as infraestruturas críticas localizadas em áreas urbanas. Delitos como furto, roubo, dano e vandalismo estão intrínsecos na sociedade brasileira, principalmente em áreas urbanas, sendo extremamente danosos as organizações públicas e privadas.

Neste diapasão, a missão do Gestor de Segurança é salvaguardar infraestruturas críticas intramuros e, também, em locais onde não possui gestão total ou parcial.

Ao refletir acerca desta missão, é importante se nortear pela doutrina do Professor Dr. Antonio Celso Ribeiro Brasiliano onde a Gestão da Segurança Baseada em Riscos (GSBR) é composta pela seguinte tríade: Ciclo de Inteligência, Cenários Prospectivos de Segurança e Gestão de Riscos em Segurança.

Seguindo este racional o Gestor de Segurança fará as seguintes entregas:

- Cenários de Riscos, Processos e Áreas Críticas para o Negócio;
- Matriz de Riscos Integrados e Incertezas Críticas;
- Riscos Críticos e Controles Chaves;
- Indicadores Estratégicos;
- Planos de Ações: Preventivos e Mitigatórios.

Convém lembrar que salvaguardar as infraestruturas críticas não é encargo exclusivo do Gestor de Segurança. Trata-se de uma atividade multidisciplinar que demanda esforços de outras áreas da Empresa e, principalmente, da alta gestão. Com isso fomenta-se, de forma muito direta, a cultura de segurança.

Portanto, o desafio de salvaguardar infraestruturas críticas de energia elétrica em áreas urbanas no Brasil somente será superado quando o Gestor de Segurança aplicar racional técnico para mapear as ameaças e oportunidades, apresentando os resultados para alta gestão e engajando outras áreas da Empresa no mesmo objetivo.

“A única coisa que podemos ter certeza, é a incerteza.”
Bauman

O ERRO “BOM”

Jefferson W. Santos Cel Av R1 MSc

Coronel Aviador da Aeronáutica (Reserva); bacharel em Ciências Aeronáuticas e Administração de Empresas, possui MBA em Gestão Estratégica de Pessoas pela FGV Brasília, Pós-graduação em Segurança e Defesa Hemisféricas pelo Interamerican Defense College (Washington – USA), Mestrado em Ciências Aeroespaciais na Universidade da Força Aérea (Rio de Janeiro- RJ) e Mestrado em Segurança e Defesa Hemisféricas pela Universidad del Salvador e Interamerican Defense College. Piloto Civil pela ANAC (Agência Nacional de Aviação Civil – Cód 138 480).

Reflexões sobre os desafios da liderança onde o “Erro bom” cometido tentando acertar e com honestidade de propósitos pode, eventualmente, ser elogiado por permitir revisão e melhorias em sistemas, processos e paradigmas.

Durante uma palestra sobre vendas dias atrás um espectador fez a seguinte pergunta ao palestrante: “Quantas vezes pode se errar? Quantas vezes o erro é tolerável? “

Bem, parece ser uma pergunta difícil e, até delicada. Diria eu: “Quantas vezes for necessário! “

Uma resposta paradoxal. Como errar pode ser necessário? Sim, é e deve ser necessário. Contudo esse erro necessário dependerá de muitos fatores, de quem lidera e de quem está errando.

Bem, falando de minha experiência como gestor e líder, após muitos anos e mais de 400 colaboradores diretos sob minha égide, sempre estimulei o erro honesto, o erro bom.

Durante reuniões e em brifings antes de voos, atividades de manutenção de aeronaves (aviões e helicópteros) ou mesmo em atividades operacionais conjuntas (outros órgãos -civis ou militares- envolvidos) eu alertava para a necessidade de não esconder os erros, por menores que fossem. O principal motivo: Investigar a causa, o fator deflagrador do erro.

Como uma organização militar tem os mesmos graus de complexidade de uma grande empresa privada (a principal diferença é a constante vigilância do Tribunal de Contas da União e Ministério Público não corriqueiras na gestão de empresas privadas) as atividades e processos sistêmicos carecem de constante acompanhamento.

Salientava naquelas ocasiões que qualquer, absolutamente qualquer ação, positiva ou negativa, em um determinado setor tinha impactos de graus diferenciados nos demais setores. Assim, um atraso, um procedimento incompleto ou feito de forma parcial oriundo no setor de manutenção tinha impactos nos setores de RH, Financeiro, Logístico, T.I, Relações Institucionais (Marketing), etc. A rigor, o mesmo ocorre nas empresas privadas.

Em aulas friso aos alunos para fugirem da "síndrome do Pequeno Príncipe" cuja melhor representatividade é ele sentado em um trono, admirando uma flor tendo ao lado uma raposa, só que em um planeta desabitado. Usava essa metáfora também nas atividades de liderança para ressaltar a importância do zelo nas atividades pois poderia prejudicar as metas de outros setores.

O ERRO HONESTO

Sempre, como líder, considerei as origens dos erros da seguinte forma (desconsidero o erro intencional):

- O funcionário não estava preparado para a atividade: Se fosse comum, a origem também envolvia os critérios de recrutamento e de seleção não adequados o que demandaria tempo e recursos para capacitação do colaborador;
- O erro aparecia de forma eventual: Meu foco ficava adstrito à problemas de ambiência, ergonômicos (uniforme, EPI, equipamentos, software, etc), problemas de instruções escritas ou faladas);
- O erro ocorria em função da atividade realizada não estar conforme com as normas e instruções escritas: Tal erro não era frequente e era "cometido" até por profissionais experientes e cuidadosos. Nesse particular era importante acompanhar o processo de atualização de diretrizes, normas, regulamentos e avisos, tanto oriundo de órgãos públicos como entidades privadas (empresas de auditoria privada, de certificações, especificações de clientes não observadas, etc). Procurava manter o foco nessas três formas de manifestação do erro. O importante é que ele precisava ser investigado, corrigido e sua incidência coibida de ser repetida.

O ERRO “NÃO-BOM”

Por cerca de dezesseis anos trabalhei no Sistema de Investigação e de Prevenção de Acidentes Aeronáuticos como Oficial de Segurança de Voo ou em outras atividades que alimentavam, diretamente, o sistema. Naquela ocasião aprendi que cerca de 90% dos acidentes e dos incidentes aeronáuticos são causados por “Erro Humano”. Por decorrência também fazia prevenção de acidentes de trabalho e o fator motivacional era o mesmo. Do que aprendi e retive como ensinamentos foram as seguintes causas de erros humanos:

- Imperícia;
- Imprudência;
- Não seguir “checklists”, normas orientadoras e diretrizes;
- Falta de preparo para identificar o erro;
- Identificar erros e condescender com eles (contornar situações de erro para não se ferir susceptibilidades). Os erros oriundos dessas práticas via de regra conduziam a um acidente ou incidente, tanto aéreo como de trabalho.

DE PDCA PARA SDCA

Portanto, salientava nos brifings e gerenciamento de atividades operacionais que em todos os processos e sistemas a ocorrência do erro é comum pois estes precisam, constantemente, ser acompanhados, avaliados, corrigidos e atualizados. Usava para esse fim, na mais singela concepção do estatístico Deming o exemplo do ciclo PDCA (Planejar, Fazer, Verificar e Corrigir) tinha sua concepção na verificação constante sobre erros que ocorriam após todo o ciclo de planejamento ser cumprido. Se o erro tivesse frequência que comprometesse a qualidade ou a produtividade, o ciclo era refeito, percorrido quantas vezes se fizesse necessário até atingir um nível de excelência ou de ocorrência de erros tolerável, quando então o processo evoluía para um SDCA, sendo o “S” de “standard” ou “padronização”.

A REALIDADE BRASILEIRA

Como toda atividade de liderança também é uma atividade de formação, orientava os líderes setoriais sob minha égide a considerarem a incidência dos fatores do macroambiente que contribuíam, sobremaneira, para existência de erros de toda sorte.

Os serviços públicos nacionais não são regulares e de qualidade questionável, tais como fornecimento de energia elétrica, transportes, telecomunicações, saneamento básico, mobilidade urbana, etc. Sobre esses serviços clientes, fornecedores e demais

setores da mesma organização tem expectativas de desempenho de um determinado setor que pode ser comprometido. Os setores dependentes deveriam se preocupar em entender a possibilidade do “erro” na promoção do produto ou do serviço antes de lançar uma crítica feroz ao setor responsável.

Da mesma forma, vivemos sob a égide de um Estado “cartorialista” profuso em leis, diretrizes, normas, avisos etc por vezes regulando uma mesma atividade em estados diferentes da federação (ex: fiscalização, tributos, etc) o que também contribui para a “existência de um erro” da empresa, sob o ponto de vista do cliente, quando um atraso ou mudança de critérios do uso do produto ou serviço ocorre.

Por fim, reconheço que em ambiente de alta competitividade, sobretudo no atual cenário de severas restrições econômicas, a tolerância para o erro reduz-se substancialmente.

Insisto, entretanto, que o erro “visível” ou declarado é uma excelente oportunidade de aperfeiçoamento de atividades, rotinas, processos e sistemas sobretudo se na organização houver o saudável hábito do “feedback” com registro e disseminação, ao longo de toda empresa, das “lições aprendidas”.

Sob essa perspectiva encareço o encorajamento de seus colaboradores e não vir a perder uma “mão de obra” não só cara, mas, também, de difícil e onerosa preparação em busca da excelência.

Pense nisso e sucesso.

CONTATOS

Jefferson Wanderley dos Santos MSc
ANAC 138.480
081 97111 0211 Vivo
081 3033 6593 (r) Vivo
@adastrapilot
www.adastrapilot.com

A IMPORTÂNCIA DA GESTÃO DE RISCOS NA PREVENÇÃO DO ROUBO DE CARGA RODOVIÁRIO

Dr. Sérgio Leônidas Dias Caldas, Cra,
MBA, MBR, CPSI, CIEIE, CIEAC, CIGR, DIDS, MSDIS, DICS
Doctor en Ciencias de la da Seguridad (Espanha) | Gestão Empresarial e Corporativa | Prevenção e Controle de Perdas | Riscos Corporativos

1. INTRODUÇÃO

O objetivo deste artigo é discorrer sobre a importância da gestão de risco na atividade logística especificamente no transporte de carga rodoviário, possibilitando que gestores que atuam nesta área possam ter uma visão da gestão de risco e como esta pode auxiliar na tomada de decisão, assim como na prevenção de perdas, preservação e maximização do ativo organizacional.

> "Maximizar o lucro sobre o capital investido na atividade logística deve ser a principal meta de uma empresa que atua no seguimento". Nesse sentido a atividade logística vem se mostrando uma ferramenta de grande importância na gestão empresarial." (BALLOU, 1993; 2003; MARTINS & ALT, 2001; BOWERSOX, CLOSS & COOPER, 2006).

Neste contexto, aumentar o lucro organizacional através da prevenção de perdas deve ser a base estratégica da gestão de risco, pois esta deve identificar onde ocorrem às maiores perdas decorrente desta atividade, seja na movimentação e armazenagem de produtos, seja no processo de aquisição de matéria prima ou até o ponto de seu consumo final. Assim a gestão de risco irá funcionar como subsidiária da atividade logística proporcionando melhores resultados financeiros e organizacionais.

Sendo assim os gestores que atual na atividade logística no transporte de carga rodoviário devem buscar mecanismos que potencializem a segurança do que será transportado, tudo com o intuito de salvaguardar o patrimônio, assim como também as pessoas, principalmente pelos riscos envolvidos nesta atividade.

Quando se fala em riscos percebe-se que nem todos os riscos são iguais. Pode-se exemplificar que um transporte de carga rodoviário não está exposto ao mesmo risco que um transporte de carga hidroviário, da mesma forma este não se equipara a um transporte de carga aéreo que cruza os continentes.

A fim de que não haja dúvida sobre o risco, Meireles (2008 apud BRASILIANO, p. 476) esclarece que:

> "O Risco também pode ser entendido como a condição que aumenta ou diminui o potencial de perdas, o risco é a condição existente de segurança ou de insegurança é que há maior ou menor chance do perigo se concretizar. Esta condição é incerta, fortuita e de consequências negativas ou danosas. Evento capaz de produzir perdas reais e mensuráveis por um padrão comum".

O risco é algo que pode trazer consequências desastrosas para as organizações, principalmente de caráter financeiro, entretanto, como se trata de algo que poderá ocorrer, cabe a gestão de risco minimizar estes efeitos, pois mesmo em caso concreto de perdas este não terá impacto tão danoso quanto por falta de um planejamento estratégico da gestão de risco. Por tanto, para que um risco incerto, fortuito de consequência danosa não cause perda financeira consideráveis nas organizações, estes devem ser minimizados, monitorados e contingenciados pela gestão de risco.

Este artigo visa dar a segurança privada que atuam na atividade logística, mas precisamente no transporte de cargas rodoviário uma visão específica da gestão de risco e, como esta pode potencializar melhores resultados para as organizações, entretanto, este conteúdo aplica-se também para os demais modais existentes possibilitando ao gestor uma melhor tomada de decisão.

Com base nisso, os gestores poderão exemplificar de forma mais clara e objetiva a alta administração quais impactos podem ocorrem em face do não investimento em segurança no transporte de carga rodoviário e quais seriam os possíveis impactos financeiros em decorrência da concretização de um roubo de carga sem a devida proteção.

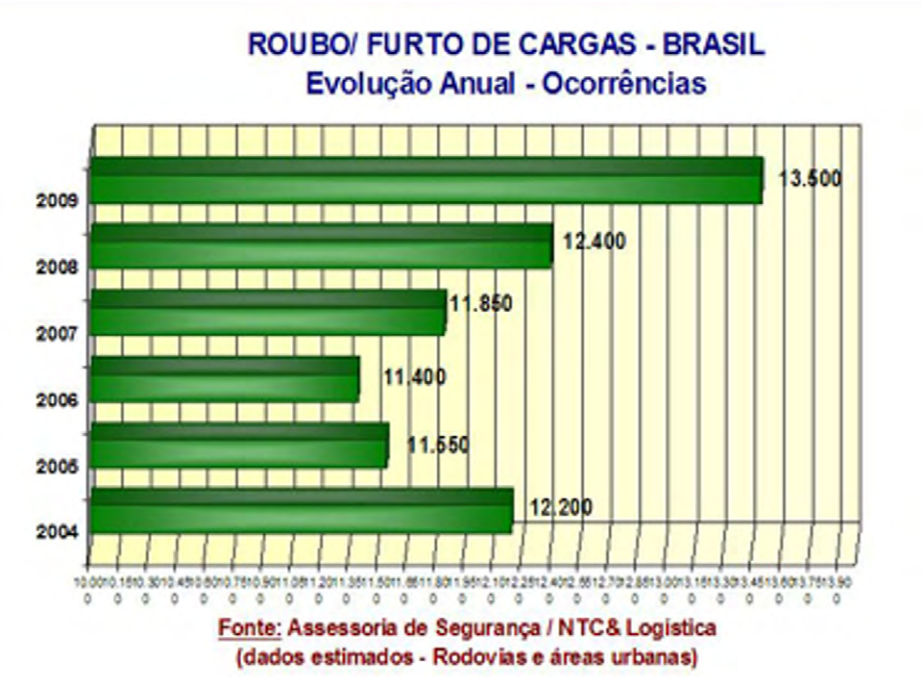
No entanto, este artigo não se considera definitivo. O trato com o grau de prescrição deste trabalho cercou-se de cuidados para não limitar a autonomia da gestão risco. Todavia, procurou-se não o descaracterizar como um documento diretriz.

A elaboração deste artigo almeja se configurar como parte de um projeto maior que vise à interação com a atividade logística na busca por ferramentas de gestão que potencializem a redução de perdas e maximização do ativo organizacional.

2. ROUBO DE CARGA NO BRASIL - GENERALIDADE

No Brasil predomina o transporte terrestre como modal rodoviário mais utilizado pelas transportadoras, com mais de 60% das mercadorias que circulam no país são via transporte rodoviário segundo dados da Confederação Nacional dos Transportes – CNT. Uma das principais dificuldades desse modal são os crimes praticados nas rodovias do Brasil aos quais citaremos alguns, a saber: roubo de carga, fraudes nos postos fiscais, corrupção policial, descaminhos, etc. Tais características fazem com que essa atividade seja acompanhada com mais efetividade pela equipe de segurança e gestão de risco, principalmente pelo valor agregado nas operações de transporte de carga rodoviário.

Estima-se que no ano de 2009 o Brasil teve um prejuízo aproximado de R$ 1 bilhão de reais com o roubo de cargas nas rodovias brasileiras, houve cerca de 13.500 ocorrências segundo dados da Associação Nacional do Transporte de Cargas e Logística (NTC & Logística). Entretanto, a realidade é ainda bem pior, pois se evidencia um crescimento em torno de 7% nos roubos de carga no Brasil ano a pós ano, conforme gráfico abaixo.

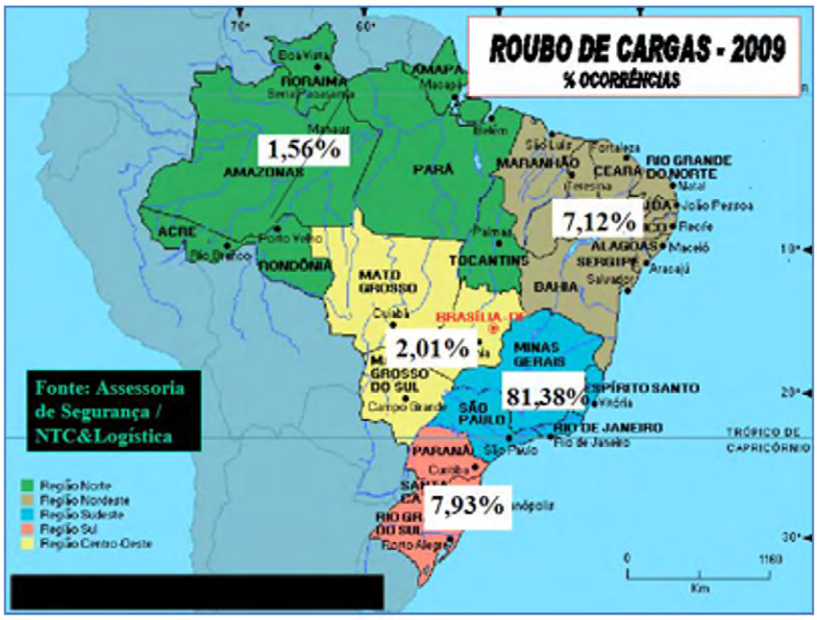


Esta prática criminosa tem impacto direto nos preços das mercadorias que circulam em todo o Brasil, uma vez que para proteger este tipo de transporte é necessário incrementos em tecnologia de segurança eletrônica, gerenciadoras de risco e seguradoras.

> “O roubo de carga no Brasil é um problema de segurança pública que se arrasta ao longo de três décadas, causando a morte de motoristas e vigilantes, milhões de reais em perdas financeiras e grandes intranquilidade no ambiente de negócios de logística em nosso país. Em razão desse cenário, outros milhões de reais são gastos com proteção de cargas armazenadas ou embarcadas para distribuição, envolvendo direta ou indiretamente centenas de empresas como seguradoras, corretoras de seguros, gerenciadoras de riscos, tecnologias de rastreamento, escolta armada e vigilância patrimonial, entre outras” (FARIAS, 2010, P. 16).

Os prejuízos vão além de R$1 bilhão, uma vez que é grande o número de casos que não são notificados. Isso acaba sendo arcado pelas empresas e seguradoras, antes de ser repassado aos consumidores.

De acordo com a estatística da NTC, 81,38% dos roubos de cargas registrados no Brasil ocorrem na Região Sudeste, isso corresponde a quase 11 mil, das 13.500 ações criminosas praticadas no país. Em valores, são cerca de R$ 660 milhões em prejuízo apenas no Sudeste. A região Nordeste consta um percentil de 7,12% com prejuízo de R$ 85,8 milhões.



Entre as mercadorias mais visadas pelos criminosos destacam-se gêneros alimentícios, eletroeletrônicas, fármacos, cigarros, têxteis, autopeças, combustíveis, além de produtos metalúrgicos e químicos.

Em face deste cenário não muito favorável, é de vital importância que os gestores tenham conhecimento a respeito da gestão de riscos, qual a sua importância para a prevenção e proteção no transporte de carga rodoviário e seu impacto caso o

aconteça. Sendo assim a gestão de riscos visa propiciar aos gestores uma melhor tomada de decisão, além de definir onde os recursos financeiros poderão ser aplicados nos transportes de carga com eficiência e eficácia, facilitando assim a mitigação dos riscos, minimização das perdas e maximização do ativo organizacional.

3. SEGURANÇA E LOGÍSTICA

> "A logística empresarial engloba todas as atividades de movimentação e armazenagem que facilitam o fluxo de produtos desde o momento da aquisição da matéria prima até o ponto de consumo final. A própria definição de logística já dar uma percepção de que furto, roubo, dano, infiltração e sabotagem são ações criminosas que podem colocar em cheque as operações logísticas de qualquer organização. Esta evidência nos indica à importância da organização desenvolver uma gestão de risco que minimizar estes e outros riscos e, em não conseguindo evitá-los, possam reagir da melhor forma possível" (Meireles, 2009, p. 109).

Sendo assim a gestão de risco na atividade logística deve minimizar os riscos em relação ao armazenamento, estocagem, distribuição e transporte, propiciando uma visão empresarial que direcione o desempenho das organizações, tendo como meta reduzir o tempo entre o pedido, a produção e a demanda, de modo que o cliente receba seus produtos ou serviços no momento que desejar. Para que esta meta seja alcançada é necessário que a empresa possua uma gestão de risco eficaz e, para que esta gestão atenda às necessidades operacionais e administrativas, é de suma importância o investimento em subsistema de segurança, não apenas estruturais, mas, sobretudo de informações informatizadas, controle de acesso e aos diversos setores e serviços da atividade logística, tendo-se sempre como norte o princípio da prioridade de proteção e parceria de trabalho em conjunto com a área de logística.

Ballou (1980, p. 66) explica que "a Logística tem como função estudar formas de se obter melhor serviço e rentabilidade nos serviços de distribuição aos clientes e fornecedores com planejamento, organização e controle do fluxo de produtos".

De fato, tais serviços especificados acima merecem por parte da gestão de risco maiores cuidados, uma vez que, são nas atividades de distribuição e fluxo de produtos onde ocorrem as maiores perdas financeiras, sejam por fraudes, furto e/ou extravios.

4. ATIVIDADE DE APOIO TRANSPORTE

O elemento de maior relevância no custo logístico é o transporte de carga, pois se refere aos vários métodos para movimentar produtos. Os sistemas básicos mais utilizados para transportes são por rodovias, ferrovias, hidrovias, aerovias e dutos.

Sendo assim os critérios a ser seguidos pela gestão de risco na escolha do modal na hora do transporte de carga, além dos riscos envolvidos de furto e roubo, devem levar em conta o produto, o custo, tempo médio de entrega, tempo de trânsito e sua variação e a análise de risco.

Nos casos em que a carga não possa ser transportada apenas pelo transporte rodoviário, a gestão de risco deve estabelecer metas para a mitigação do risco em casos de outros modais, os quais devem envolver a redução do custo total, redução do tempo de trânsito em longos percursos, redução do impacto ambiental, redução do congestionamento nas rodovias e melhora do nível de serviço, além da segurança pessoal em relação ao corpo laboral envolvido.

> O principal problema do transporte de carga no Brasil é a distorção da matriz de transporte. Um país com dimensões continentais que deveria ter os modais ferroviários e aquaviário como os principais meios de transporte, tem no modal rodoviário a sua maior alternativa de transporte com um percentual de 60% da carga transportada (MEIRELES, 2007, p. 2).

Apesar de que os maiores risco no transporte de carga rodoviário estejam ligados a roubo, outras ameaças têm sido presente nesta atividade: apropriação indébita, acidentes com colisão, tombamento e deslizamento de carga, avarias, estragos ou perecimento de produtos e contaminação ambiental por produtos químicos. Esses fatores são maximizados em virtude do péssimo estado de conservação das rodovias do Brasil.

Essa realidade faz com que a gestão de risco na atividade de transporte de carga rodoviário tenha um papel de maior relevância, uma vez que é ela quem irá apontar a utilização de recursos de segurança a fim de mitigar o risco e potencializar maior proteção ao bem que será transportado. Para tanto, a utilização de tecnologias como rastreadores de veículos e cargas através do Global Positioning System (GPS) se faz necessário. Ao lado deste subsistema, pode ser utilizada a escolta armada, alternativa que deve ser precedida de uma avaliação criteriosa do trinômio **custo X benefício X risco**, dentre outros.

5. GERENCIAMENTO DE RISCO

> “É a adoção de um conjunto de técnicas e medidas preventivas que visam identificar, avaliar e evitar ou minimizar os efeitos de perdas ou danos que possam ocorrer no transporte de mercadorias, desde a origem até o destino da carga, garantindo que o produto esteja no local desejado, dentro do prazo previsto e de acordo com sua conformidade” (SOUZA, 2010, p. 1).

O conceito de gerenciamento de risco dá a dimensão da responsabilidade da gestão de risco em face do cenário brasileiro desfavorável de transporte de carga rodoviário, pois como observado há diversas formas crimes e perdas nesta atividade, sejam elas diretas (roubo) ou indiretas (extravio, fraudes etc.). Sendo assim a gestão de risco deve estabelecer um plano de gerenciamento de risco que vise potencializar melhores resultados organizacionais em face dos perigos existentes nesta atividade.

> "A gestão de risco deve estabelecer ainda objetivos específicos no plano de gerenciamento de risco, os quais devem conter a redução dos riscos, preservação de vidas humanas e bens materiais, viabilização de seguros adequados às atividades operacionais da empresa, cumprimento dos compromissos com clientes, diferencial competitivo no mercado, aumento da produtividade e lucratividade, manutenção da imagem da empresa e motivação dos funcionários" (FARIAS, 2010, P.2).

Em decorrência desta atividade tão competitiva e acirrada nos dias atuais, se faz necessário que as organizações invistam continuamente na segurança de seus bens transportados com base nos objetivos de gerenciamento de risco aqui enunciados, caso contrário, sem uma gestão de risco eficiente, perdas serão inevitáveis.

6. RISCOS OPERACIONAIS

Os riscos nas operações logísticas mais comuns a qualquer atividade empresarial as quais não poderão ser desconsideradas na análise de risco são respectivamente:

> "Roubo de carga (embarcada ou armazenada), avaria da carga (decorrente de acidente no transporte ou sinistro no armazém como inundação, incêndio e/ou desabamento), acidente ambiental (decorrente do derramamento de produtos químicos transportados em áreas de mananciais), acidente automobilístico (decorrente da combinação de fatores como a negligência ou imprudência do motorista, das más condições das estradas e/ou das más condições meteorológicas), bloqueio da estrada (decorrente de fenômeno natural como deslizamento de terra, queda de ponte, inundação), manifestação sociais (greves; movimento dos sem-terra, índios), greve (movimento sindical que paralisa os motoristas e os carregadores, ou ainda os agentes alfandegários) e naufrágio (acidente no transporte fluvial ou marítimo de carga, decorrente das más condições climáticas e até por ações "piratas)" (FARIAS, 2010, p.2).

Seja qual for o tipo de análise de risco (matemático ou subjetivo) utilizada pela gestão risco, o principal objetivo é garantir que o produto desde sua origem, armazenagem, movimentação, transporte e entrega ao cliente final seja feita da melhor forma possível e segura, tudo com o fito de se obter melhor resultado operacional, administrativo e financeiro.

Nos casos em que apesar da análise de risco tenham sido favoráveis ao transporte de carga rodoviário e, mesmo assim, por questões fortuitas a ação humana na proteção dos bens transportados possa ocorrer alguma forma de perda, são importantes três ações de contramedidas da gestão de risco como forma de preservação do ativo organizacional, a fim de minimizar os efeitos de uma crise estabelecida em um fato concreto como por exemplo de roubo de carga.

> "Medida de Intervenção Direta - são ações imediatas de intervenção sobre o sinistro em andamento. Que vão desde o bloqueio do veículo de carga e o acionamento de apoio dos órgão governamentais (policia, bombeiro, SAMU etc.), até o envio de veículo para transbordo da carga e a ativação do Comitê de Crise que a empresa deve estabelecer em sua política de Gestão de Risco; Medidas de Limitação da Crise – significa estabelecer os limites da crise e não permitir que se estenda além destes, compartimentando as consequências por meio de ações de contenção. Proteger o nome da empresa cobrindo o logotipo da mesma no veículo, retirar o uniforme do motorista e acionar a assessoria de imprensa; Medidas de Restauração da Operação – são as medidas que visam retornar as operações afetadas pela crise, no menor tempo possível. O transbordo da carga para outro veículo e a continuidade da viagem, ou a transferência da carga de um armazém afetado para outro mais seguro, ou ainda a troca do motorista que não esteja em condições de seguir viagem, entre outras de acordo com cada crise" (FARIAS, 2010, p.2).

Estas são algumas medidas de gerenciamento de risco que podem ser adotas no transporte de carga rodoviário, todavia, cada empresa deve estabelecer seu plano de gerenciamento de risco com base nas análises estabelecidas, necessidades, critérios de riscos envolvidos e de acordo o contexto do negócio da atividade logística.

7. A GESTÃO DE RISCO E A ISO 31000

Pode-se observar que quando se fala em gerenciamento de risco vimos logo à importância que ela tem em todo o processo logístico, mais precisamente no transporte de carga rodoviário.

> “O foco no transporte de carga não é à toa, ocorre que cerca de 60% dos custos da logística está no transporte. Sendo assim, os custos em decorrência de perdas nesta atividade trás impacto direto para toda sociedade e não apenas para as transportadoras, gerenciadora de risco e seguradoras, pois estas perdas acabam por ser repassadas para os consumidores finais” (MORETTI, 2010, p. 20).

Com o advento da ISO 31000 o gerenciamento de risco deve ser organizado a partir do framework (estrutura) de processos proposto pela norma no qual visa à estruturação da gestão de riscos nas organizações. Apesar de que a ISO 31000 não apresente os métodos que devem ser utilizados para a identificação dos riscos, análise de risco e monitoramento dos riscos os quais serão somente apresentados na ISO 31010, todavia, ela dá a estrutura de como fazer a gestão e apresenta os processos que cada gestor de risco pode seguir, utilizando as ferramentas já existentes e utilizadas hoje, pois nenhuma delas foi invalidada.

A ISO 31010 traz em sua norma, 28 tipos de análise de gestão de risco os quais as organizações podem escolher a melhor forma que se adapta ao seu negócio. Desta forma cada gestão de risco poderá mensurar seus riscos e suas perdas em decorrência de sua atividade final.

Qualquer que seja o método de análise de risco utilizado pela gestão de risco no transporte de carga rodoviário, este deve mensurar de forma clara e objetiva quais os impactos financeiros e possíveis perdas podem ocorrer em decorrência desta atividade. Sendo assim, pode-se citar o método Brasiliano que tem contribuído de forma decisória junto às organizações de transporte de carga rodoviário onde os recursos financeiros devem ser investidos de forma a proteger o ativo organizacional, proporcionando melhores resultados financeiro.

Embora o custo da perda em um caso concreto de roubo de carga via rodoviário seja percebido apenas do total da carga subtraída, é importante ressaltar que há outros custos envolvidos os quais não são percebidos por muitas organizações e que devem ser levados em consideração.

Para exemplificar outros custos em decorrência de um roubo de carga rodoviário, Moretti (2010, p. 21) propõem a seguinte equação de perda:

CP= Sp + St + Cc + Rc – (I-P)

I. **CP** – custo da perda

II. **Sp** – é a substituição permanente do produto, aquilo que foi efetivamente roubado.

III. **St** – é a substituição temporária, ou seja, os recursos gastos com a

operacionalização de substituir temporariamente o caminhão, motorista, pedágios, frete, e tudo que foi gasto para atender a ocorrência.

IV. **Cc** – é o custo consequente, que é a perda gerada em decorrência da ocorrência, que pode ser, em muitos casos, maior do que o valor da carga, por exemplo a perda de um cliente.

V. **Rc** – é a redução do dinheiro em caixa, que neste caso só será contabilizado o dinheiro, em espécie, caso tenha sido roubado ou se também era transportado.

VI. **I** – é a indenização que o seguro pagará, caso a carga seja segurada.

VII. **P** - é o prêmio pago pelo seguro até o momento da ocorrência e sabemos que o valor é maior devido ao tipo de carga e a quantidade de ocorrência existente.

De fato, o custo da perda em decorrência de um sinistro logístico vai muito além da perda do produto roubado incluindo desde o não cumprimento dos prazos acordados com o cliente até a sua necessidade, quando não for atendida. Assim a análise de risco juntamente com uma gestão de risco alicerçada com a ISO 31000 dá aos gestores que atuam neste seguimento oportunidade concretas de análise de risco com foco na excelência operacional na busca por ferramentas de gestão que auxiliam a tomada de decisão na hora de escolher qual a melhor forma de se transportar um bem material no transporte de carga rodoviário.

Contudo, apenas a análise e gestão de risco não resolvem os problemas destacados. É preciso que as transportadoras, gerenciadoras de risco e operadores logísticos invistam continuamente em recurso tecnológicos de segurança, tanto para a proteção de seus veículos quanto para os centros de distribuição – CD's ou locais de armazenagem. Deve-se investir na infraestrutura dos referidos locais de forma que está propicie ao corpo operacional maior segurança, bem-estar e conforto durante a operacionalização dos produtos e serviços dispostos nestes ambientes. Ressalta-se que a qualidade desta atividade depende da integração dos profissionais de logística e segurança para a melhoria contínua dos serviços oferecidos aos clientes.

8. CONCLUSÃO

Diante do que foi exposto neste artigo pretendeu-se apresentar uma revisão conceitual em logística e segurança, bem como a abrangência da Gestão de Riscos no Transporte de Carga Rodoviário e de como este pode contribuído para o sucesso das operações logísticas no Brasil, quando bem executado, com foco na redução das perdas e maximização do ativo organizacional.

Destaca-se o referencial teórico-bibliográfico, na qual percebe-se que a gestão de riscos tem caráter preventivo nas organizações e este direciona o tratamento dos riscos que possam causar perdas ou danos à empresa, tratamento esse que engloba os objetivos e contramedidas de proteção bem como a cobertura securitária quando for o caso.

Além disso, ainda sob essa ótica tratou-se neste documento identificar no modal rodoviário onde ocorrem as maiores perdas e de como estas podem ser evitadas a partir das análises da gestão de risco com base nos cenários históricos e prospectivos de ocorrência no Brasil.

Neste contexto, a gestão de risco por meio das análises de histórico de ocorrência ou cenário prospectivo pode apresentar medidas eficazes de prevenção, pois normalmente, tais medidas requerem investimentos financeiros em tecnologia e treinamento para o corpo operacional da segurança e logística. Além de que é necessário um planejamento estratégico consistente e uma relação custo X benefício adequada para obter, da alta administração, o apoio e os recursos necessários para implementação das medidas preventivas no transporte de carga rodoviário.

Outras medidas também possuem sua relevância pelos reflexos na organização, que normalmente envolvem mudanças comportamentais, operacionais, tecnológicas e comerciais na atividade logística e que tende a agregar ao corpo funcional da empresa uma melhor produtividade e eficácia operacional.

O mais importante da gestão de risco é direcionar a alta administração a utilizar os recursos financeiros na proteção do transporte de carga rodoviário da melhor forma possível otimizando e potencializando a produtividade da operação logística sem comprometer a eficácia operacional e produtividade do corpo laboral.

No entanto, só terão sucesso no Brasil, mas precisamente no transporte de carga rodoviário, as empresas que continuamente investem em segurança física, humana, eletrônica e, que principalmente esteja alicerçados em uma gestão de riscos que tenha em sua essência o planejamento estratégico da gestão de risco pautado em objetivos concretos de mitigação dos riscos, redução das perdas, preservação e maximização do ativo organizacional com a finalidade de trazes a esta atividade maior segurança, bem estar e conforto organizacional.

REFERÊNCIAS

BALLOU, Ronald H. - Gerenciamento da cadeia de suprimentos: planejamento, organização e logística empresarial. 4° Ed. Porto Alegre: Bookman, 2003.

BOOWERSOX, CLOSS E COOPER. Gestão logística da cadeia de suprimentos. Porto Alegre: Makron Books, 2006.

BRASILIANO, Antonio Celso Ribeiro. Gestão e Análise de Risco Corporativo: Método Brasiliano Avançado. São Paulo: Sicurezza, 2009.

FARIAS, Carlos. Segurança na Cadeia Logística. Como Funciona o Gerenciamento de Crise em Operações Logísticas. Ano 17, Nº 188, Abril 2010. São Paulo: Jornal da Segurança.

MARTINS, Petrônio Garcia, ALT, Paulo R. Campos. Administração de Materiais e Recursos Patrimoniais. São Paulo: Saraiva, 2001.

MEIRELES, Nino Ricardo. Manual do Gestor de Segurança Corporativa. Salvador: Étera, 2008.

MEIRELES, Nino Ricardo. Processos e Métodos em: Prevenção de Perdas e Segurança empresarial. 1º Ed. São Paulo: Sicurezza, 2010.

MEIRELES, Nino Ricardo. Sistema de Segurança. Salvador: Étera, 2006.

MORETTI. Cláudio dos Santos. Segurança na Cadeia Logística. A Importância da Gestão de Risco no Transporte de Cargas. Ano 17, Nº 188, Abril 2010. São Paulo: Jornal da Segurança.

SOUZA. Paulo Roberto. O Gerenciamento de Riscos no TRC. Disponível online em: <http://www.ntcelogistica.org.br/gris/gerenciamento.asp>. Acesso em 14. Nov. 2010.

“BRINCANDO COM A SEGURANÇA II”

Cristiano Pazzini Lobo Lazzarotti, MsC, CPSI,
Especialista em Segurança, Riscos, Emergências e Crises empresariais.
Diretor da CP Assessoria e Consultoria e DA CEAS-Brasil para o Estado de Minas Gerais.

Há treze anos, escrevi o artigo “Brincando com a Segurança” que, na época, por ser um tema de grande interesse público, pelo aumento da criminalidade no Brasil, principalmente furtos e roubos a residências e comércios, foi amplamente publicado em vários jornais e revistas de renome e circulação nacional.

O foco do artigo era mostrar a sensação de insegurança e, consequentemente a busca indiscriminada, sem quaisquer critérios técnicos, por sistemas de segurança física e/ou eletrônica. Com isso, o mercado de segurança privada e de segurança eletrônica cresceu assustadoramente.

Em virtude desse crescimento desordenado, surgiram os “aventureiros”. Diversos profissionais como: chaveiros, eletricistas e instaladores de interfone, passaram a vender kits de segurança (alarmes, câmeras, sensores, cercas-elétricas, entre outras parafernálias). Magazines, lojas de materiais de construção também passaram a comercializar sistemas de segurança tornando-os “produtos de prateleira”.

Assustados e desamparados, os propensos clientes começaram a instalar cercas elétricas, alarmes e câmeras de segurança em seus comércios e residências. Ao passarmos por uma rua, observamos claramente o “modismo da segurança”, pois quase todas as residências e lojas possuíam algum tipo de dispositivo de segurança.

De 2008 até hoje, o que mudou?

Mudou bastante. A criminalidade aumentou, a impunidade imperou principalmente para os crimes considerados de menor potencial ofensivo, as Forças de Segurança Pública continuam trabalhando incansavelmente. Com isso, a busca por sistemas de segurança cresceu ainda mais, o preço dos dispositivos ficou mais acessível e surgiram milhares de novas empresas e aventureiros no segmento de segurança.

A preocupação com esse modismo permanece, pois, os riscos continuam incalculáveis e irreversíveis. E o pior, não são percebidos por quem adquire dispositivos de segurança, por falta de conhecimento e técnicas agressivas de vendas.

A soma de diversos fatores podem potencializar ainda os riscos aos quais essas pessoas estão expostas.

Por que quando estamos doentes, vamos ao médico? Quando temos um problema jurídico, consultamos um advogado? Quando o carro apresenta um defeito, levamos ao mecânico? Quando realizamos o sonho de construir a tão sonhada casa, contratamos arquiteto e engenheiro? Não seria, então, mais correto contratarmos um especialista em segurança (devidamente habilitado e certificado) quando buscamos soluções para nossa segurança?

“De nada adianta comprar uma parafernália de equipamentos eletrônicos, instalar cercas cortantes e outros dispositivos se não sabemos quais são nossos reais riscos (externos e internos) e nem o que realmente precisamos proteger”.

GESTÃO DE RISCOS EMPRESARIAIS EM NOSSO TEMPO – UMA OPINIÃO

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI,
General de Exército da Reserva, é Vice-Presidente de Operações
de Consultoria da empresa Brasiliano INTERISK

A diversidade e a complexidade das ameaças hoje presentes no ambiente de negócios conferem à tarefa de gestão de riscos um caráter eminentemente profissional.

Não se admite mais, como costumava ocorrer até há bem pouco tempo, que a alta direção do negócio espere a ameaça tornar-se perfeitamente delineada para só então tomar medidas destinadas a enfrentá-la. Também é difícil compreender que sistemas de gestão de empresas importantes ainda se valham de planilhas para registrar, analisar e planejar o enfrentamento dos riscos.

O mundo evoluiu depressa em termos de disponibilidade de sistemas baseados na ciência, tecnologia e inovação (CT&I), para o bem e para o mal. Assim é que, a par das inimagináveis facilidades colocadas pela evolução científico-tecnológica à disposição dos administradores, não é menos real o sem-número de armadilhas que lhes assombra o caminho – armadilhas essas preparadas com a utilização de meios da mesma natureza. Isso para falar apenas do risco cibernético, aquele que vem merecendo ultimamente a maior cobertura em nossos meios de comunicação.

A nova realidade no ambiente de negócios, após os lamentáveis episódios de ataques cibernéticos à empresa Colonial Pipeline, nos EUA, e a diversas grandes empresas e órgãos de governo no Brasil e em muitos outros países, não é de molde a deixar tranquilo nenhum gestor consciente de suas responsabilidades. Tudo que não se pode admitir neste momento é a existência do CEO avestruz, aquele que venda os olhos para não ter que fazer face à realidade que se lhe impõe sem dó nem piedade.

A súbita notoriedade conferida aos ataques cibernéticos não nos deve fazer esquecer dos tradicionais, e nem por isso menos importantes, riscos patrimoniais, de segurança de pessoal, instalações, processos e assim por diante. Também não podemos negligenciar os modernos riscos à confidencialidade, integridade e disponibilidade dos dados, frequentemente interligados ao risco cibernético, assunto que assumiu relevância sem precedentes com a entrada em vigor da Lei nº 13.709, de 14 de agosto de 2018, a LGPD.

Antes de mais nada, é preciso pensar de forma holística, de modo a integrar toda a gestão de riscos num único arcabouço que, uma vez alimentado de forma competente por uma equipe de profissionais bem-preparados, ofereça respostas rápidas e eficazes às ameaças e às oportunidades. O modelo das três linhas de defesa, apoiado em um software abrangente e de fácil manuseio, é sem dúvida uma solução de excelente qualidade.

Nesse campo de atuação, o preparo intelectual dos profissionais em todos os níveis é essencial. É necessária uma ampla capacitação que incorpore desde os gestores do mais alto nível até os operários do chão de fábrica, de modo a que todos se conscientizem da natureza das ameaças e dos cuidados que devem tomar para evitá-las. Liderança, neste como em tantos outros momentos, é a palavra-chave.

Não estamos falando aqui da necessidade de investimentos milionários e que por si sós tenham o condão de inviabilizar a empresa. As soluções simples são muitas vezes as mais eficazes. Não há, porém, como deixar de realizar alguns investimentos, tanto na capacitação do pessoal quanto na contratação dos serviços de empresa confiável da área de gestão de riscos, que realmente aponte as falhas a serem corrigidas e não apenas diga o que a alta direção da empresa gostaria de ouvir. Além disso, será necessário o aporte de recursos destinados à aquisição de equipamentos de proteção individual (EPI), de equipamentos diversos e softwares atualizados que permitam minimizar as fragilidades e vulnerabilidades da empresa em todas as áreas.

O essencial é que, mesmo na eventualidade de sofrer um sinistro, seja ele de que natureza for, a empresa possa continuar em atividade para realizar as entregas necessárias e cumprir, ainda que com dificuldade, os compromissos assumidos. Para isso, o mesmo software deve propiciar a elaboração do Plano de Continuidade de Negócios (PCN), uma espécie de salvo-conduto da empresa, um roteiro para seguir adiante, mesmo nos momentos mais difíceis.

No mundo em que vivemos, há quem diga que nossa única certeza é a mais absoluta incerteza. Pessoas responsáveis precisam lidar com a imprevisibilidade para levar a bom termo as tarefas colocadas sobre seus ombros em relação à família, à empresa em que trabalham, à sociedade de que são parte atuante. Implantar um bom modelo de gestão de riscos em suas empresas será certamente um passo acertado nesse caminho.

SEGURANÇA FÍSICA E PATRIMONIAL HOSPITALAR: GESTÃO E PLANEJAMENTO

Cândido Brasil

Especialista em Segurança Física e Patrimonial, com ênfase em gestão na área hospitalar. Formação Acadêmica em Processos Gerenciais. Pós-Graduação em Gestão de Segurança Pública e Privada. Pós-Graduação em Gestão Hospitalar. Experiência em área administrativa, liderança de equipes, controle de custos e qualidade, planejamento e implantação de projetos corporativos, palestrante e instrutor em cursos de extensão e formação de profissionais na área da saúde.

GESTÃO: A Segurança Física e Patrimonial Hospitalar (SFPH) é parte de um sistema de grande complexidade, que envolve cuidado com a vida, saúde, emoções, valores morais, financeiros e patrimoniais, e sua participação neste ambiente deve incluir planejamento e profissionais capacitados para atuarem em qualquer posto e em qualquer evento de crise que venha surgir.

No cenário ideal, a gestão do setor (departamento) de SFPH da instituição deve participar dos processos decisórios da organização, opinando tecnicamente sobre os impactos dos projetos internos sobre a segurança e o gerenciamento de riscos na organização.

Suas observações e apontamentos certamente reduzirão as chances de insucesso desses projetos, sejam eles estruturais, de implantação de equipamentos de controle ou comunicação e contratação de profissionais especializados, evitando gastos e conflitos desnecessários, assim como o retrabalho e perda de tempo com profissionais e valores financeiros.

O Gestor de Segurança Física e Patrimonial Hospitalar deverá ter bom senso na administração das questões rotineiras e extraordinárias que surgirem, visto que o setor trabalha com o imprevisível e é sistematicamente pressionado com opiniões e sugestões de pessoas que não possuem o conhecimento técnico da função. Isto vale para qualquer profissional da Segurança Patrimonial.

A formatação e estruturação de um departamento de SFPH eficaz é difícil, pois depende muito da forma com que a alta administração da organização enxerga esse processo, ou seja, se julga basicamente que a segurança é custo ou investimento, se a trata com a importância que merece ou apenas uma função que identifica “cara e crachá”.

Por isto são importante o conhecimento técnico e o controle emocional para o desenvolvimento do trabalho. Saber o momento de ouvir e ou absorver críticas e sugestões, assim como a firmeza para agir e indicar as melhores soluções para o dia a dia e eventos que possam surgir, além de administrar o seu corpo funcional e todos os conflitos que lhe atingem: qualificação, falta de efetivo, escalas de férias e folgas, afastamentos, estrutura tecnológica, uniforme e outros correlatos.

A questão da gestão da SFPH é tão relevante que está presente em dois dos principais manuais de acreditação internacional: o da Organização Nacional da Acreditação (ONA) e o da Joint Comission International (JCI), que possuem capítulos dedicados a gestão de segurança em ambientes hospitalares, o que demonstra a importância desse processo para essas organizações.

PLANEJAMENTO: É preciso ressaltar a importância da SFPH nas organizações hospitalares pelo fato incontestável de que esses ambientes são suscetíveis a muitos riscos, decorrentes de comportamentos humanos, acidentais ou intencionais, e de fenômenos naturais. Estes riscos necessitam de uma atenção preventiva, com planejamento e medidas pró-ativas para o seu controle e atuação em caso de necessidade.

O ambiente hospitalar é uma estrutura multiforme por compreender diversas especialidades de trabalhos como hotelaria, lavanderia, serviços médicos, vigilância, restaurantes, recepção e atendimento a pacientes, acompanhantes, visitantes, fornecedores etc.

Tais peculiaridades favorecem o risco de ocorrências como: casos de alto fluxo de desconhecidos, fuga de pacientes, roubo de medicamentos, furtos de pertences institucionais ou pessoais, sequestro de incapazes, agressões verbais e físicas, resgate, suicídios, assassinatos... e ainda risco de contaminação biológica, incêndios, explosão, pane elétrica, desabamentos e outros.

Além dos riscos citados, em muitas organizações há o desrespeito dos próprios funcionários da instituição para com os profissionais da segurança, no controle de acessos e identificação, na uniformização e no cumprimento das normas institucionais internas.

A segurança física e patrimonial hospitalar não pode ser tratada de forma amadora, mas sim de maneira metódica, de modo com que todos os elementos que compõe sua estrutura estejam unidos e visem expandir a metodologia implantada a fim de aperfeiçoar a capacidade de identificação dos riscos e ameaças que exijam a adoção de medidas pró-ativas e práticas.

A implantação de um sistema de segurança eficiente no âmbito hospitalar terá sucesso se houver uma excelente combinação dos recursos humanos e materiais na busca dos objetivos propostos e para isto uma forte política de segurança deve ser elaborada e divulgada extensivamente nos setores distintos envolvidos na laboração hospitalar, desta forma gerando uma cultura de segurança, com participação coletiva fundamental nas ações que visem impedir um ato delituoso.

Um planejamento eficiente deve seguir alguns preceitos, que podem e devem variar de acordo com o nível de segurança que a direção da unidade hospitalar requer, acrescentado do endomarketing, que é um item fundamental que não deve ser esquecido, visto que a segurança só pode ser empreendida com sucesso contando com a participação do todo, ou seja, público interno e externo.

O endomarketing atua objetivando especificar ao corpo funcional, de todas as áreas, a real necessidade da implantação das medidas e protocolos de segurança, informando o papel de cada um e a sua importância no processo.

Através da coletividade ciente e qualificada pode-se assegurar a segurança das pessoas, do patrimônio, da informação e dos processos basilares da organização.

O marketing externo ocorre de forma paulatina, compassada, progressiva e contínua com os usuários do sistema hospitalar a fim de estabelecer alguns itens essenciais na área de segurança, tais como: horários para visitas aos pacientes, número de visitantes, troca de acompanhantes e o uso de materiais de identificação como crachás, etiquetas ou pulseiras, salientando a real necessidade de o ambiente hospitalar possuir uma política de segurança estabelecida e transparente.

Para o sucesso na implantação de um bom projeto de Segurança Física e Patrimonial Hospitalar, deve-se levar em conta alguns requisitos básicos, tais como:

1) Análise territorial – Estudo do local onde o a estrutura física do predial (Hospital) está construída, com suas características periféricas: índices criminais da região, presença das forças de segurança pública, sazonalidades locais, meios de transporte etc.;

2) Análise de riscos – Identificação dos riscos puros (aquele ocorrido antes da prevenção, ou seja, a ameaça efetivada sem a providência de nenhuma medida para evitá-la) sujeitos a ocorrer no desenvolvimento do projeto;

3) Diagnóstico dos sistemas de proteção – Atenuação de cada risco identificado;

4) Indicação dos sistemas de gerenciamento de crises e emergências – Ocorrência dos sintomas dos riscos apurados;

5) Controle de qualidade e produtividade – Apuração dos indicadores de todas as ações, normas e procedimentos adotados.

A credibilidade do setor de Segurança Física e Patrimonial em um ambiente hospitalar depende muito do grau de envolvimento, colaboração e atuação efetiva das demais áreas que formam o público interno, que precisa ser incluído nas medidas de segurança determinadas e instigados a participar do processo. Para se atingir estes objetivos é fundamental uma segurança direcionada a um sistema integrado com todas as áreas da unidade hospitalar, vindo assim a gerar uma sensação de segurança para funcionários e usuários, com proteção aos bens patrimoniais da organização e pessoais dos indivíduos, especialmente os relacionados à vida e contribuindo para um ambiente sadio e protegido.

A SEGURANÇA AÉREA

Jefferson W. Santos Cel Av R1 MSc

Coronel Aviador da Aeronáutica (Reserva); bacharel em Ciências Aeronáuticas e Administração de Empresas, possui MBA em Gestão Estratégica de Pessoas pela FGV Brasília, Pós-graduação em Segurança e Defesa Hemisféricas pelo Interamerican Defense College (Washington – USA), Mestrado em Ciências Aeroespaciais na Universidade da Força Aérea (Rio de Janeiro- RJ) e Mestrado em Segurança e Defesa Hemisféricas pela Universidad del Salvador e Interamerican Defense College. Piloto Civil pela ANAC (Agência Nacional de Aviação Civil – Cód 138 480).

As reflexões que seguem tratam da Segurança no contexto aéreo sem, todavia, se adstringir somente às questões de segurança específicas de prevenção, de enfrentamento de sinistros, de sequestros e de eventos correlatos. É a situação na qual não há insegurança e onde os efeitos e os agentes adversos podem ser previstos, plotados, eliminados ou terem seus danos mitigados.

Os aspectos básicos que serão considerados ao se tratar de Segurança versarão sobre a identificação, a prevenção e a atuação corretiva oportuna para se eliminar os riscos ou se mitigar os resultados indesejados.

Agentes, fatores e eventos adversos geram a adversidade, ou seja, a situação na qual, mesmo havendo planejamento e gestão para eliminar ou reduzir seus impactos, eles ocorrem.

Para se atender, portanto, à proposta da elaboração do presente artigo faz-se necessário dividir o complexo universo da atividade aérea para se entender e atuar preventivamente.

Serão, com este objetivo, oferecidas considerações que seguem abaixo e que são fruto de experiência prática como investigador de acidentes aeronáuticos e de trabalho em um período de dezesseis anos como oficial de carreira na Aeronáutica.

Tais reflexões também tem estofo na especialização aquinhoada pelo autor ao longo de mais de cinco mil horas de voo em dezesseis tipos de aeronaves diferentes,

incluindo helicópteros mono e bimotores além de experiência por mais de quatro anos em operações offshore, com pousos em navios, em plataformas, em hotéis flutuantes e em refinarias.

Ante o acima exposto e para efeito de uma compreensão mais ampla e fluída, considerar-se-ão os seguintes aspectos:

- Segurança Aérea;
- Segurança Aeronáutica; e
- Segurança Aeroportuária.

Em todos três aspectos acima (contexto aéreo) alguns fatores estão presentes como causas deflagradoras principais dos eventuais danos. São eles:

- Um objeto fora do solo;
- O “centro de gravidade” desse objeto;
- A amarração ou fixação desse objeto; e
- A fixação das plataformas aéreas (acima do solo) ou de meios de deslocamentos desse objeto.

Convém, antes de se prosseguir com as presentes reflexões, reenfatizar-se que a perspectiva de Segurança em comento abrange, a partir da noção da “perda”, a prevenção de prejuízos advindos de indenizações, ou de multas ou de interdições das atividades na empresa na ocorrência de acidentes envolvendo pessoas ou patrimônios.

Em particular, ao tratar-se de um acidente fruto de uma “insegurança” após qualquer aeronave (avião ou helicóptero) sair do solo, seu retorno incontrolável causará sinistros na ordem praticamente incomensurável de indenizações pecuniárias. Imagine-se, para facilitar o entendimento, uma aeronave caindo após a decolagem em uma área deserta, ou em casas ou sobre hospitais ou, ainda, sobre depósitos de combustível.

A SEGURANÇA AÉREA

Destarte, ao tratar-se de Segurança Aérea observa-se a **FIXAÇÃO** do objeto ou elemento que ficará ***fora do solo.*** Nesta categoria são considerados:

- Teleféricos, gruas, trilhos suspensos para deslocamentos de ganchos suspendendo motores, pallets etc. (comuns em armazéns de estocagem e em oficinas de manutenção veicular, ou de aviões, de geradores e similares);

A prevenção ocorre planejando-se sinalizações e isolamento de áreas restritas à circulação -de pessoas ou de veículos- ao longo do percurso desses elementos em elevação e, ao redor, em suas cercanias imediatas. Enfim, a preservação da vida e de patrimônio é o objetivo principal dessas medidas preventivas.

Apesar de já fixado e, ainda, necessariamente fora do solo, o foco das atenções se dará no CENTRO DE GRAVIDADE. Então, nesta categoria tem-se:

- Drones, balões, dirigíveis, aeronaves, helicópteros etc.

Estes artefatos (ou veículos aéreos) dependem, sobremaneira, de uma distribuição de carga que atenda às especificações acerca do “passeio” (deslocamento) do centro de gravidade (os manuais de operação apresentam tais características e restrições);

Encerrando-se este quesito depreende-se que a Segurança Aérea depende, sobremaneira, de fixações e de rigorosa observância da integridade do centro de gravidade.

A SEGURANÇA AERONÁUTICA

Já sob esta perspectiva, observa-se que aeroportos e campos de pouso são locais de operação de embarques e de desembarque e, também, de carga e descarga de objetos e bagagens. Da mesma forma, há circulação de aeronaves, de veículos para abastecimento e para eventuais manutenções das aeronaves. Também ali transitam tratores rebocando pranchas para bagagens e cargas, escadas e pequenas usinas geradoras de energia (para serviços de limpeza, de comissaria, de manutenção nas aeronaves ou para auxílio no acionamento dos motores).

Os riscos à segurança -além da guarda e da vigilância de bens e de patrimônios- são ampliados por falta de prevenção comuns quando nesses tipos de aeroportos ou de aeródromos não se tem a presença de agências de vigilância sanitária, de postos de saúde e de operações de atendimentos de ambulâncias, evacuação aero médica no caso específico de navios, embarcações, plataformas, hotéis flutuantes etc.

Enquadram-se, portanto, nesta categoria:

Helipontos, pistas de pouso, navios, prédios sem a estrutura de um aeroporto (para militares do corpo de bombeiros, ambulâncias, evacuação aero médica etc.)

SEGURANÇA AEROPORTUÁRIA

Agora focando-se nesta nova caracterização de estruturas para atividades de pousos e de decolagens, tem-se:

- Helipontos, pistas de pouso, navios, prédios que contem com a estrutura de um aeroporto (corpo de bombeiros, ambulâncias, evacuação aero médica, agências de polícia (municipal ou estadual) etc.)

Cada elemento físico ou predial ou área requer uma abordagem específica para efeitos de prevenção de segurança. Desta forma não só na prevenção de acidentes aeronáuticos devem ser prevenidos, mas também existe a passibilidade de se deparar com outros tipos de sinistros ou subtrações. Aliados a esse possível cenário, podem tais áreas podem estar suscetíveis a atos de terrorismo sendo estes afetos, especificamente, s às intervenções de profissionais das Secretarias de Segurança Pública ou do Corpo de Bombeiros.

Por fim, à guisa de um redirecionamento, a abordagem acerca da Segurança Aérea (com os condicionantes de se estar “fora do solo” foram tratados com o foco ampliado apesar do caráter introdutório para se estimular reflexões mais amplas sobre esta nova abordagem.

A experiência profissional à frente de equipes multifuncionais em setores onde a prevenção sobre aspectos ligados à Segurança era fundamental, evidenciou que a ampliação e sedimentação dos conhecimentos acerca do negócio da empresa, o domínio do conhecimento de todos os fatores e das variáveis que, eventualmente, podem interferir na consecução dos objetivos da empresa, a capacidade de se coletar dados e informações fidedignas e o mérito de disseminá-las dentre os membros da força de trabalho amplia, sobremaneira, o portfólio, a expertise e a confiabilidade da empresa nesta matéria.

Espera-se, desta forma, ter se contribuído com uma reflexão e uma abordagem inovadora sobre Segurança Aérea.

SEGURANÇA HOSPITALAR: NA FRENTE DA LINHA DE FRENTE

Cândido Brasil

Especialista em Segurança Física e Patrimonial, com ênfase em gestão na área hospitalar. Formação Acadêmica em Processos Gerenciais. Pós-Graduação em Gestão de Segurança Pública e Privada. Pós-Graduação em Gestão Hospitalar. Experiência em área administrativa, liderança de equipes, controle de custos e qualidade, planejamento e implantação de projetos corporativos, palestrante e instrutor em cursos de extensão e formação de profissionais na área da saúde.

Com o advento da pandemia mundial surgida em razão da COVID-19, o mundo inteiro viu-se impotente frente a esta ameaça invisível sem cor, cheiro, classe social ou ideologia e que possui alto nível de transmissão entre os seres humanos. No front da luta contra este inimigo letal, estão os profissionais da saúde, que passaram a ter o merecido reconhecimento pela importância de suas abnegadas ações na defesa da vida, na dedicação ao cuidado individual do paciente, até à exposição aos riscos inerentes a esta nova situação, atuando, muitas vezes, sem as condições ideais de trabalho, tanto estrutural quanto de proteção individual.

Diariamente a mídia tem destacado o trabalho louvável de médicos, enfermeiros, técnicos e auxiliares de enfermagem no tratamento de pacientes, diante das complicações ocasionadas pelo coronavírus, justificando plenamente a missão da área fim no ambiente hospitalar. Sem deixar de valorizar a importância fundamental e o trabalho louvável destes profissionais, vale lembrar que existem outros atores que laboram na complexa engrenagem de uma instituição hospitalar, atuando na área meio, com o objetivo de propiciar as melhores condições de trabalho para o sucesso no tratamento de pacientes e alguns destes trabalhadores estão “na frente da linha de frente”, tão propagada atualmente, considerando serem eles os primeiros a terem o contato direto com o enfermo.

No ambiente hospitalar, mesmo antes da alteração da rotina devido a pandemia, o primeiro contato do paciente na sua chegada para o atendimento individual sempre foi com a Segurança Física e Patrimonial Hospitalar (SFPH) nas portarias e na sequência

pela recepção que realiza o cadastro, para depois prosseguir na triagem, frente a enfermagem, ao médico e aos cuidados de técnicos e auxiliares. Este acolhimento também pode ocorrer no estacionamento ou entradas paralelas, na chegada emergencial de ambulâncias da SAMU ou de empresas privadas e até mesmo de veículos particulares.

São os profissionais desta categoria, muitas vezes invisível, mas sempre presentes, que atuam a fim de manter a ordem, buscando promover a tranquilidade necessária para o paciente, acompanhantes e servidores, durante o período de consulta ou mesmo internação, mantendo uma postura de permanente em observação, cientes de que toda e qualquer ação é constantemente analisada pelo público, tanto externo quanto interno, incluso as categorias profissionais que atuam em cada unidade hospitalar, conforme suas características, sejam elas clínicas, traumatológicas ou materno-infantil.

O serviço da SFPH engloba ações por todos os espaços físicos de uma instituição, com presença em locais abertos, como pátio e estacionamento, até áreas de consulta, exames, internação e de acesso restrito, como UTI's, salas de recuperação, maternidade e outros, mantendo contato direto com funcionários, usuários, acompanhantes e prestadores de serviço, geralmente expostos a todo tipo de contágio. Entre suas atividades estão o controle do fluxo de usuários, a observação do deslocamento individual de pessoas, a vigilância do patrimônio institucional, a prontidão permanente, aliada a técnica para abordagens e contenções, o contato direto com as forças de segurança pública em fatos que fujam a normalidade, entre outras,

A SFPH diferencia-se das demais pela sua especificidade de atuação, acolhedora e informativa, preventiva e de observância, presencial e virtual, devendo ser exercida por profissionais credenciados, com conhecimento técnico adquirido através do curso de formação e aperfeiçoamento homologado pelo Departamento de Polícia Federal e independente da constituição das equipes, sejam elas terceirizadas ou orgânicas, seu desempenho deve seguir os objetivos estratégicos da instituição, resultando na manutenção da normalidade no ambiente hospitalar, gerando além de uma sensação de segurança, um sentimento de bem estar a todo público interno.

A SFPH trabalha sempre com o imprevisível, independente de situações adversas à população, sejam pandemias, epidemias ou outros eventos, buscando resguardar a instituição e seu patrimônio, funcionários, usuários e acompanhantes, mantendo a sua posição, "a frente da linha de frente", em defesa da vida e da saúde.

COMO AS EMPRESAS PODEM OBTER UMA VISÃO ANTECIPADA E DE ADAPTAÇÃO AOS ATAQUES CIBERNÉTICOS?

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CEGRC, CIEAC, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE e MBS.

\Doutor em Ciência e Engenharia da Informação e Inteligência Estratégica pela Universit Paris – Est (Marne La Vallée, Paris, França); presidente da Brasiliano INTERISK

A detecção de sintomas de ataques cibernéticos a sistemas empresariais, abrangendo tanto TI (Tecnologia da Informação – Nível Corporativo) quanto TO (Tecnologia Operacional – Nível Industrial e Operações de Negócio) a tempo de as empresas acionarem suas defesas e em paralelo realizarem a análise de como o ataque poderá ser materializado, aí incluída uma projeção dos prováveis impactos, de modo a reduzi-los mediante um eficaz gerenciamento dos incidentes, passou a ser um desafio estratégico para os gestores da segurança cibernética, informação e privacidade - CIP.

As empresas necessitam ser resilientes às ameaças cibernéticas e para isso necessitam estruturar respostas adequadas ao perfil de ataques que poderão sofrer. Isso significa que a percepção de sintomas de que há algo anormal nas redes e sistemas é um fator crítico de sucesso. Mediante uma antecipação bem-sucedida, as empresas podem estruturar muito mais assertivamente suas defesas cibernéticas e também gerenciar as respostas adequadas aos incidentes. Um Plano de Resposta a Incidentes bem estruturado, com o emprego de cenários prospectivos de ataques cibernéticos é o grande diferencial para mitigar consequências.

Hoje, as empresas encontram-se submetidas a pressões intensas, tanto oriundas da área externa quanto da área interna: da área externa, as ameaças crescem de forma exponencial, incidindo sobre um perímetro estendido (sem fronteira definida, na verdade), perpetradas por hackers cada vez mais capacitados; já as pressões vindas da área interna devem-se principalmente à insuficiência orçamentária (resultado da não conscientização da alta gestão) e da carência de recursos humanos capacitados,

o que redunda na falta de agilidade de antecipação e de resposta.

Na verdade, a segurança cibernética deve estar à frente dos hackers para poder prevenir e mitigar os ataques. Esse é o grande desafio. Na figura a seguir, demonstramos graficamente essas pressões.

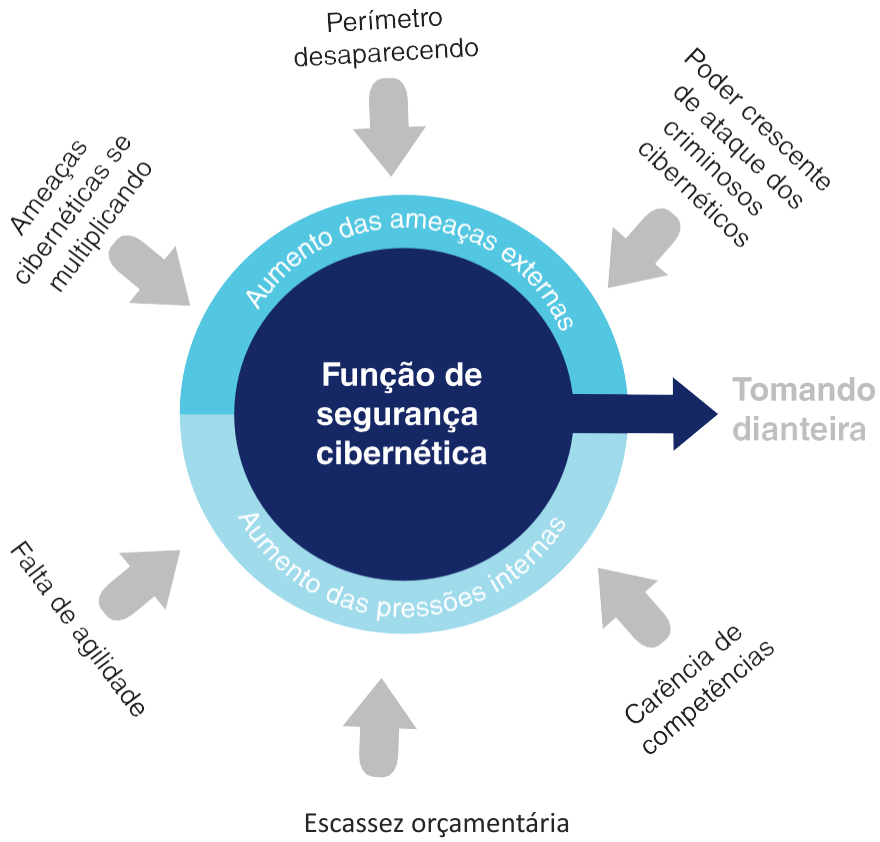


Figura 1: Pressões da Segurança Cibernética
Fonte: Metodologia da Brasiliano INTERISK – Construção de Cenários de Ataques Cibernéticos

Para fazer face a ameaças cada vez mais sofisticadas, a empresa deve dispor de uma capacidade muito forte de detecção, visando entender como os ataques cibernéticos podem ser materializados, bem como a estratégia empregada e o vetor de ataque utilizado. Para isso, deve entender muito bem suas próprias vulnerabilidades e saber qual o perfil de um possível agressor. Deve também identificar, sob a ótica do hacker, que tipo de vantagem sobre a empresa ele (hacker) poderá ter, caso o ataque obtenha sucesso. O diagrama de causa e efeito a seguir mostra as perguntas que devem ser respondidas pelos gestores da CIP (Cibernética, Informação e Privacidade), de modo a obter a visão antecipada do evento.

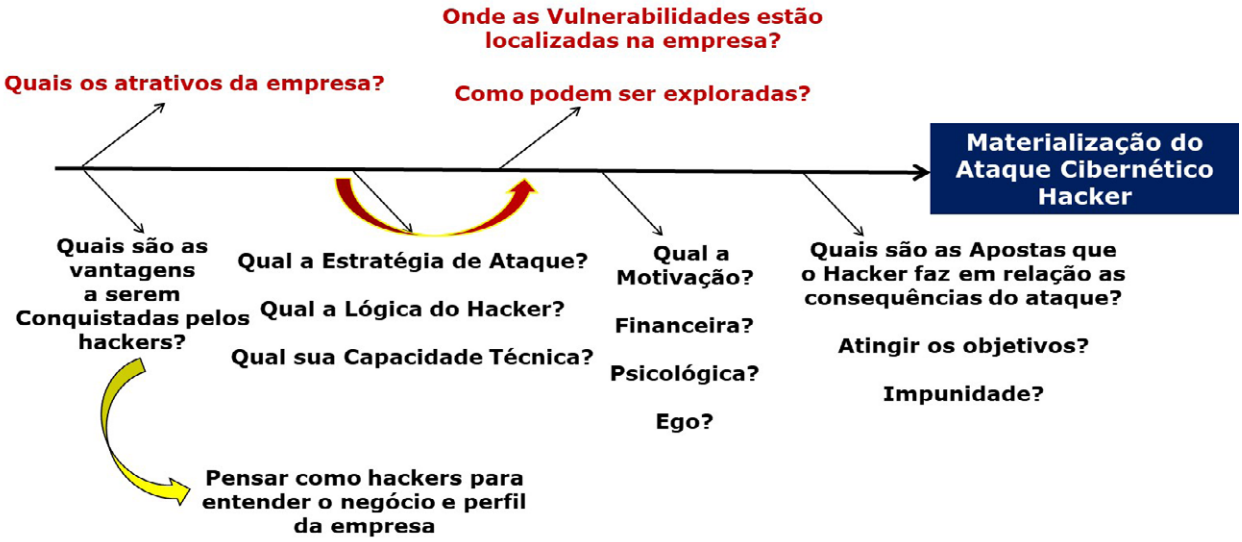


Figura 2: Diagrama de Causa e Efeito para ataques cibernéticos
Fonte: Metodologia da Brasiliano INTERISK – Construção de Cenários de Ataques Cibernéticos

Portanto, antes de pensar em tecnologia as empresas devem pensar em antever os modi operandi do agressor, bem como o seu perfil.

Desta maneira, a empresa, para ter cyber resiliência com muita agilidade, deve percorrer três fases em seu processo de atuação preventiva e mitigatória. São elas:

Figura 3: As fases dos ataques cibernéticos
Fonte: Metodologia da Brasiliano INTERISK – Construção de Cenários de Ataques Cibernéticos

1. DETECÇÃO

É a capacidade das organizações de prever e detectar ameaças cibernéticas. As organizações precisam realizar um trabalho de inteligência com foco nas ameaças cibernéticas e nas medidas de defesa ativa para prever quais ataques estão sendo orientados em sua direção e detectá-los quando eles estiverem próximos, antes que

sejam bem-sucedidos. A empresas precisam ter dados sobre o que vai acontecer e para isso devem contar com um trabalho de inteligência analítica sofisticada que lhes proporcione um alerta antecipado quando situações anômalas estiverem ocorrendo no tráfego da rede ou no sistema.

2. DEFESAS E SEGURANÇA

Os mecanismos de defesa de segurança formam basicamente o escudo de defesa, a muralha que o hacker tentará vencer. Tudo começa com a determinação do grau de risco que a empresa está preparada para enfrentar, tendo em vista o levantamento e a avaliação de cenários de ataques cibernéticos de toda a sua superfície de ataque. Em seguida emprega as três linhas de defesa:

- **Primeira Linha:** encarregada de executar medidas de controle nas operações do dia a dia;
- **Segunda Linha:** responsável por implantar funções de monitoramento contínuo pelo SOC – Security Operation Center (Centro de Operações de Segurança), incluindo o SIEM – Security Information and Events Management (Gerenciamento de Segurança da Informação e Eventos), em toda a infraestrutura de TI da empresa, aí incluídos os sistemas de segurança, controles internos e Cyber Security Risks Assessment (Avaliação dos Riscos e Cenários Cibernéticos);
- **Terceira Linha:** Responsável por exercer uma forte e independente auditoria interna.

3. REAÇÃO

Caso a Detecção não funcione (a organização não percebeu a chegada da ameaça) e haja uma falha na Defesa de Segurança (as medidas de controle não eram fortes o suficiente), as empresas precisam estar preparadas para lidar com a provável interrupção das operações e para gerenciar a crise, ter devendo dispor de uma pronta capacidade de resposta a incidentes.

Elas também precisam estar preparadas para preservar provas de maneira segura, do ponto de vista forense, e, em seguida, investigar a violação, a fim de satisfazer partes interessadas cruciais, como clientes, reguladores, investidores, autoridades policiais e o público em geral, qualquer uma das quais poderia mover ações por perdas e danos ou por descumprimento de obrigações. Caso as partes responsáveis pelo incidente sejam identificadas, a empresa poderá mover processos contra elas.

Finalmente, elas também precisam estar preparadas para retornar à rotina de negócios o mais rapidamente possível, ou seja, recuperar o quanto antes o costumeiro

ritmo das operações. Aprender com o incidente é crucial para que a empresa não volte a cometer as mesmas falhas, daí a necessidade de registrar todas as ações realizadas e o grau de eficácia nelas obtido no sentido de conter, erradicar e recuperar.

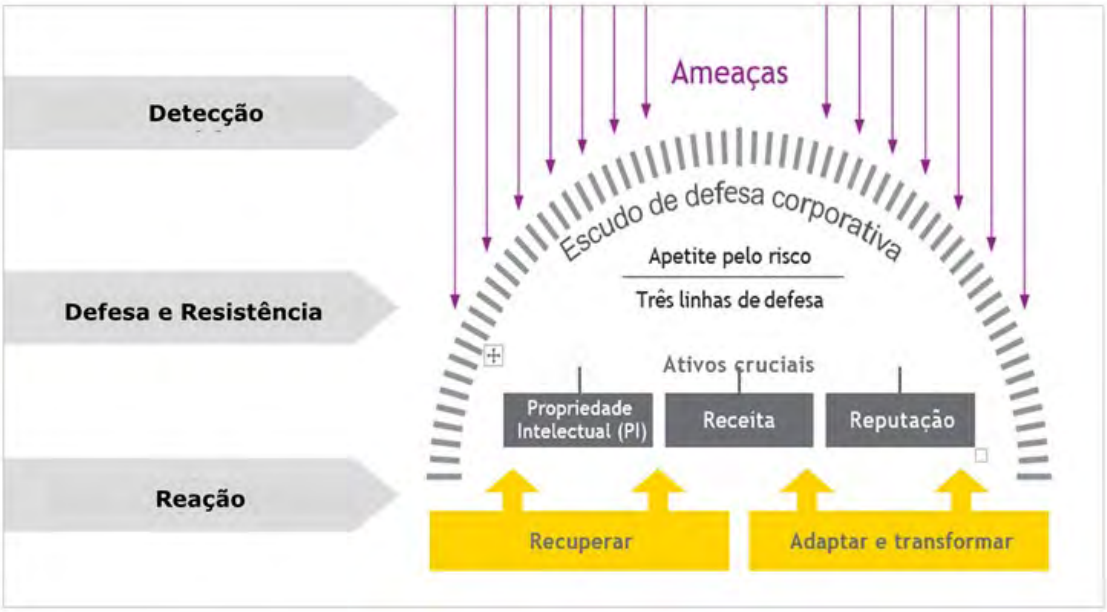


Figura 4: Fases dos ataques cibernéticos – Visão Esquemática. Fonte: Metodologia da Brasiliano INTERISK – Construção de Cenários de Ataques Cibernéticos

Em função disso, é cada vez mais importante correlacionar as informações e, assim, garantir a segurança dos negócios, através da inteligência analítica.

Mas como fazer isso na mesma velocidade em que aparecem novas ameaças e um turbilhão de informações para serem gerenciadas? A resposta é adotar plataformas de segurança inteligente. Elas se tornaram um elemento fundamental na estratégia de segurança das áreas da Cibernética, Informação e Privacidade – CIP para gerenciar estes desafios, possibilitando detecção e respostas automáticas e emitindo dashboards e relatórios que permitirão às empresas identificar, realizar a triagem e atuar de forma mais eficaz durante os incidentes.

Porém, adotar uma nova ferramenta e ter uma abordagem prospectiva impõe desafios aos líderes das empresas. Para enfrentar esses desafios, ou pelo menos os mais importantes dentre eles, cumpre à Alta Administração responder às seguintes perguntas:

- Como manter os especialistas da empresa atualizados e motivados?
- Como garantir a nova plataforma rodando de forma plena?
- A empresa faz uso de todo o potencial da nova plataforma? Ou usa apenas parte do seu potencial?

- Adianta a empresa ter visibilidade das ameaças e não ter um time 24×7 atuando nos incidentes?
- A empresa acompanha de forma direta os novos modi operandi dos hackers em outros países?
- A empresa está adicionando inteligência ao seu sistema de segurança CIP e aos seus processos?

Todas essas dúvidas nos mostram que essas plataformas, por si sós, não atingem os resultados necessários para garantir a proteção dos dados. É preciso contar com um parceiro especializado em segurança CIP que forneça serviços do tipo SOC, agregando processos e conhecimentos maduros, além de um time de especialistas nessa tecnologia, com analistas de segurança que atuem 24 horas por dia, 7 dias por semana, assegurando que nenhum incidente de segurança identificado pela solução passe despercebido ou deixe de ser triado e tratado.

A detecção de ameaças e de violações de conformidade em tempo aceitável e a capacidade de gerenciar incidentes com o mínimo de impacto certamente farão diferença no desempenho do negócio.

Garantir segurança para o negócio não pode ser um mero exercício de especulações. Se não tiver consciência plena de quais são as Joias da Coroa (aquilo que é crítico, relevante e essencial) do negócio e não concentrar o foco na proteção ao redor delas, a empresa poderá pagar o preço por cenários de ataques cibernéticos que não estão no radar. A consequência será massiva, prejudicando os setores operacional, legal e financeiro, além da imagem da empresa.

Possuir a visão de antecipação e adaptação é o grande desafio para os líderes empresariais neste século XXI.

VAZAMENTO DE DADOS: UMA REALIDADE BRASILEIRA! VOCÊ SABE COMO PREVENIR E MITIGAR ESTE RISCO?

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CEGRC, CIEAC, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE e MBS.

Doutor em Ciência e Engenharia da Informação e Inteligência Estratégica pela Universit Paris – Est (Marne La Vallée, Paris, França); presidente da Brasiliano INTERISK

Em uma pesquisa feita pelo Procon-SP foi constatado que maioria desconhece a legislação de proteção de dados. Pouco mais que sete mil pessoas responderam ao levantamento, mas somente 35% declararam conhecer a Lei Geral de Proteção de Dados – Lei federal nº 13.709, criada para organizar e disciplinar as relações entre os titulares dos dados e aqueles que os coletam e fazem uso destes, garantindo regras claras e segurança.

Esta é uma grande vulnerabilidade, que mostra a falta de sensibilização das pessoas em relação ao tratamento de segurança de seus dados pessoais e pessoais sensíveis.

Na pesquisa foi perguntado se os consumidores conheciam a Lei Geral de Proteção de Dados - LGPD

Levando em consideração a quantidade total de consumidores que responderam ao questionário, somente 35% disseram ter conhecimento da LGPD, ao contrário dos 65% que disseram não conhecer. Aqueles que disseram conhecer, foi pedido que apontassem alternativas com afirmações sobre a legislação, sendo que apenas uma com informações totalmente corretas sendo ela: “LGPD é uma lei que protege os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural”. No qual apenas 20% optaram por essa alternativa.

As outras opções eram: 1ª “LGPD é uma lei que protege os dados pessoais coletados dentro e fora do território nacional”, alternativa escolhida foi de 58; 2º “É direito do titular ter acesso às informações sobre o tratamento dos próprios dados, que deverão

ser disponibilizadas de forma clara. Contempla só o tratamento de dados que estão fora da rede (off-line)", questão apontada por 11 e 3ª "LGPD é uma Lei que cuida exclusivamente da nossa segurança na internet", opção assinalada por 10%.

A Lei Geral de Proteção de Dados é uma legislação que protege os dados pessoais coletados em território nacional e que regulamenta o tratamento de dados coletado tanto online quanto off-line.

Os consumidores também foram questionados se já tiveram conhecimento de que algum dado seu foi vazado, compartilhado indevidamente ou mesmo roubado. A grande maioria, equivalente a 73% não teve conhecimento de vazamento de seus dados, mas um percentual considerável, 30% tiveram.

Dos 32% tiveram conhecimento ao ser vítima de um golpe; 17% souberam ao investigar após ver notícia sobre vazamento de dados; 8% ao ter o nome sujo indevidamente; 6% tiveram conhecimento por amigos ou parentes; 2% ao ser indevidamente processado civil ou criminalmente; e 35% souberam de outra forma.

A grande maioria de dados vazados foi de documentos pessoais como RG, CPF, CNH, carteira de trabalho entre outros, em segundo lugar vieram dados cadastrais de lojas virtuais e em terceiro lugar dados bancários por exemplo: nº conta, nº cartão, senha etc.

O que isto significa? Há uma necessidade de troca de atitude, mindset, pois se não houver sensibilização sobre segurança de seus próprios dados, imaginem o que ocorre com dados das empresas. Portanto campanhas de conscientização são primordiais para diminuir a chance de os dados pessoais vazarem.

Na verdade, o Data Loss Prevention – DLP, termo em inglês, tornou-se assunto recorrente entre os executivos C-Level das empresas. Os incidentes relacionados com este tema inquietam profundamente e movimentam as áreas de Tecnologia da Informação, Cibernética e de Segurança Corporativa, sem falar em Recursos Humanos. As consequências com a perda de informações estratégicas e ou dados sensíveis, em função de requisitos legais, LGPD, impactam massivamente as empresas em termos financeiros, além da reputação em seu mercado.

Mesmo assim, diante deste cenário poucas empresas executam campanhas estruturadas de endomarketing. Grande maioria acredita que basta implantar um sistema, realizar uma palestra e com isso suas informações estão seguras.

Afinal o que você entende como Prevenção Contra Vazamento de Informações ou no linguajar da área Data Loss prevention – DLP?

Nós da Brasiliano INTERISK definimos a Prevenção contra Vazamento de Informações como sendo um conjunto importante de políticas, métodos e tecnologias utilizadas para tentar evitar que dados estratégicos ou sensíveis – quesitos legais – sejam

compartilhados indevidamente, subtraídos da empresa ou enviados para ambientes inseguros ou manipulados por usuários não autorizados.

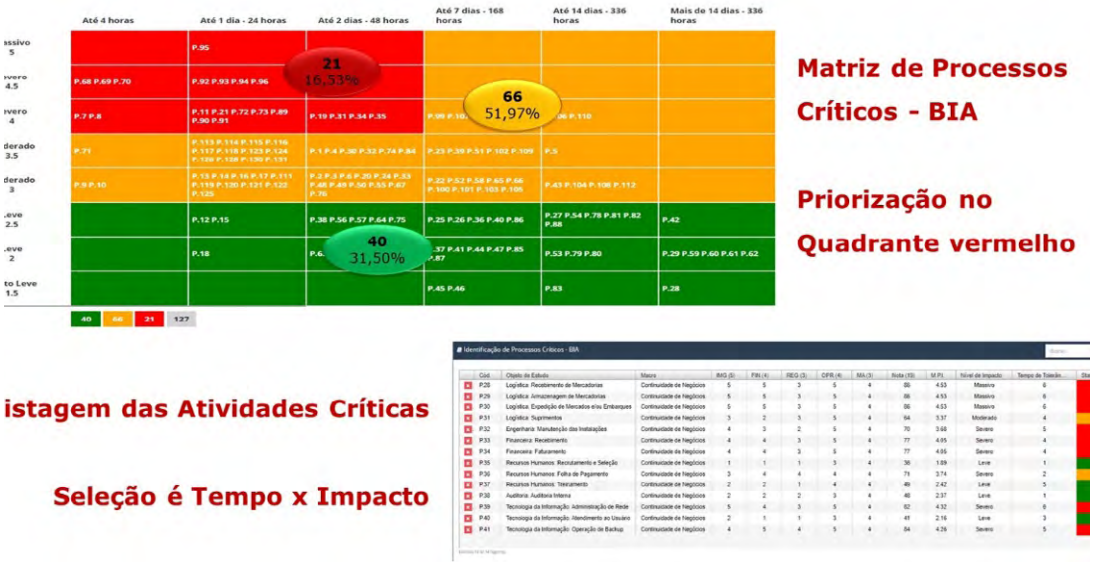
A empresa deve entender que para evitar o DLP vir a se concretizar tem que aceitar o fato de que as informações e dados estratégicos e dados pessoais e pessoais sensíveis podem ser conseguidos de forma voluntária ou involuntária. Isso mesmo. Se um funcionário de médio escalão possui uma informação estratégica e não sabe o valor desta para a empresa, grande possibilidade de vazar através de conversas informais com grupos de amigos, ou mesmo ser vítima de engenharia social e ou técnica de indução.

Para isso a empresa deve ter um Processo Estruturado Contra Vazamento de Informações, com metodologia e critérios parametrizados. A Brasiliano INTERISK possui um processo estruturado simples e prático, onde temos que seguir os seguintes passos:

PRIMEIRO PASSO

A empresa precisa identificar, na sua cadeia de valor quais são os processos críticos que suportam o “core” do negócio. Estes processos devem merecer toda atenção do pessoal de segurança da informação, cibernética e segurança corporativa.

Pode-se utilizar como critério e parâmetro o BIA – Business Impact Analysis, onde medimos as consequências em termos de vazamento e sua falta nas tomadas de decisões e ou em processos de negócio.



Acima temos um exemplo, onde os processos localizados no quadrante vermelho são estratégicos e ou sensíveis.

SEGUNDO PASSO

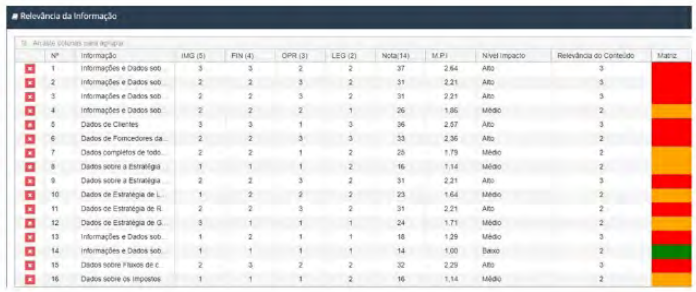
Este segundo passo é o mais estratégico e importante, pois a empresa deve classificar as informações pelo seu conteúdo estratégico e também pelos requisitos legais. Ressalto que grande parte das empresas mundiais, cerca de mais de 85%, não praticam este segundo passo. A classificação das informações deve constar da Política de Segurança das Informações, onde está classificação irá demandar proteção diferenciada.

A classificação das informações não tem um critério definido, mas em termos de benchmarking pode-se classificá-las em quatro níveis:

1. Informações confidenciais – o mais alto nível;
2. Informações ou dados restritos – médio nível de confidencialidade;
3. Uso Interno – o mais baixo nível de confidencialidade – público interno da empresa sabe da informação;
4. Informações e dados são públicos – todos podem ter a informação.

Informações classificadas, estas devem ser rotuladas e tratadas conforme sua política, podendo até integrar o IP da máquina, o e-mail do usuário para saber se ele pode mandar esta informação para fora da empresa. Aí o sistema de proteção de dados funciona. Percebem que se a empresa não classificar as informações, os sistemas de nada adiantarão.

Listagem de Informações das Atividades e ou Processos Críticos



Critério:

Impacto

(imagem – financeiro – legal – operações)

X

Relevância

(estratégico – tático –operacional ou requisito legal)

17	Dados e Informações sob...	2	2	3	3	33	2,36	Alto	2	
18	dados e informações do I...	2	2	3	3	33	2,36	Alto	2	
19	Dados sobre a Estratégia ...	3	2	3	3	38	2,71	Alto	3	
20	Dados e Informações do I...	2	2	3	2	31	2,21	Alto	3	
21	Inventário do acesso lógic...	2	3	3	2	35	2,50	Alto	2	
22	Dados e Informações do ...	2	2	2	2	28	2,00	Médio	1	
23	Dados e Informações sob...	2	1	2	1	22	1,57	Médio	2	
24	Dados e informações sob...	2	1	1	1	19	1,36	Médio	1	

Acima um critério que utilizamos para identificar informações ou dados estratégicos

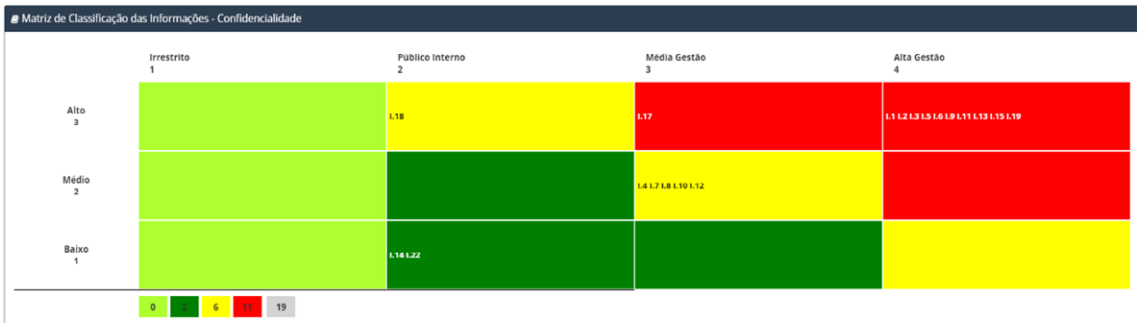
Estas informações, para melhor visualização, vão para uma Matriz de Relevância:

Matriz de Relevância das Informações das Atividades Críticas da Empresa

Priorização das Informações das Atividades e ou Processos Críticos

Quadrante Vermelho

Com as informações estratégicas e sensíveis identificadas, podemos classificá-las, utilizando sua relevância versus sua confidencialidade, este cruzamento vai para outra, a Matriz de Classificação de Informações e Dados:



É uma Matriz que de forma direta, ao cruzar os dois parâmetros, automaticamente já tenho o nível de tratamento desejado pela sua importância.

Temos que saber também neste passo, qual a característica das informações e dados, em relação a sua movimentação, ou seja, saber se elas estão:

Resultado da Classificação:

4. Quadrante Vermelho: Confidencial

3. Quadrante Laranja: Restrito

2. Quadrante Verde: Uso Interno

1. Quadrante Verde Claro: Público

A Matriz é fruto do cruzamento dos Critérios:

Criticidade para o Negócio

x

Nível de Divulgação e Acesso

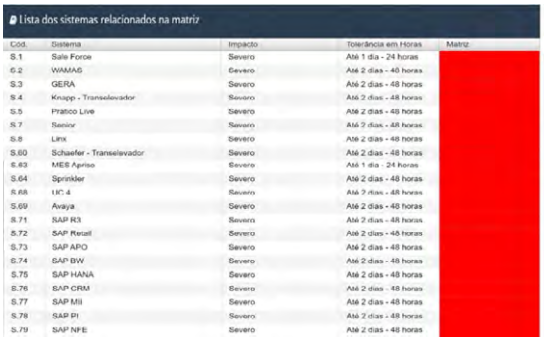
- Em uso nas máquinas dos usuários;
- Em movimento na rede corporativa ou fora dela;
- Se estão armazenadas, como por exemplo em servidores.

A característica da movimentação irá direcionar a demanda da segurança necessária destas informações.

TERCEIRO PASSO

Com base nos processos críticos para o “core” da empresa, as informações e dados classificados quanto sua confidencialidade, aí é necessário identificar quais são os Sistemas de Tecnologia da Informação que sustentam os dois pilares. Uso também para selecionar o inventário de sistemas, o BIA – Business Impact Analysis.

Abaixo um exemplo de utilização do BIA para sistemas.



Listagem dos Sistemas Que apoiam as Atividades Críticas

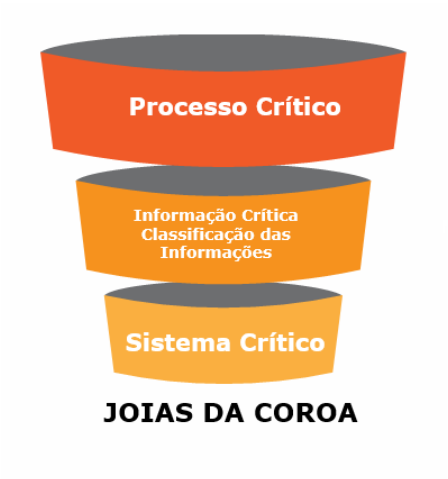
Critério de Seleção:

Tempo x Impacto

Bem teoricamente, estou com minhas Joias da Coroa protegidas, certo? Errado!

Ainda falta o elo mais crítico deste sistema.

Falta o Fator Humano!!



QUARTO PASSO

Este quarto passo significa identificar quais são as pessoas, e não o cargo, que manipulam ou tem acesso a estas informações. Temos que saber o nível de maturidade destas pessoas. Isso mesmo! Temos que fazer uma avaliação e identificar seus pontos fracos nos quesitos:

Engenharia Social; Técnicas de Indução; Phishing; Controle de senhas – de que forma controla e nível de complexidade; Nível de Segurança de seu computador ou aparelho mobile: criptografado, utilização de senhas, entre outros; Nível de tratamento com Segurança de documentos físicos: leitura em locais públicos, deixa o documento em cima de mesas, poltronas, salas de reunião, etc; Segurança digital - Trabalha em locais públicos com computador e aparelhos mobile; Segurança de Redes: utiliza redes abertas públicas tais como hotéis, aeroportos.

Qual a importância de sabermos a Maturidade sobre Confidencialidade das Informações destas pessoas sensíveis e estratégicas para as empresas?

A importância é identificar estas fraquezas e tratá-las, para evitar que sejam alvos de possíveis agressores. Podemos montar uma régua, com base nos oito quesitos e termos um range de maturidade. Régua para sabermos o nível de maturidade, para classificar as pessoas e treiná-las nos quesitos considerados fracos. Abaixo um exemplo desta classificação:

Classificação da Maturidade das Pessoas com Acesso a Informações Confidenciais

	Nome		Redes Sociais	Engenharia S...	Phishing	Controle de S...	Nível de Segu...	Nível de Trata...	Segurança Di...	Segurança de...	Soma Notas	Criticidade
	João Alves		2	2	1	2	2	2	2	2	15	
	Carlos Antunes		1	2	2	3	2	3	2	3	18	
	Maria Clara		3	2	2	2	2	2	2	2	17	
	Joana Vinicius	ra	1	1	1	1	1	1	1	1	8	
	Mário Ferraz		1	1	1	1	1	1	1	1	8	
	Cláudio Fernandez	s	3	3	3	3	3	3	2	2	22	
	Saturnino dos Santos	tica	2	2	2	2	2	2	2	3	17	
	Priscila Alves		3	3	3	3	3	2	2	3	22	
	Roberto Carlos	s	3	1	3	3	3	3	3	3	22	

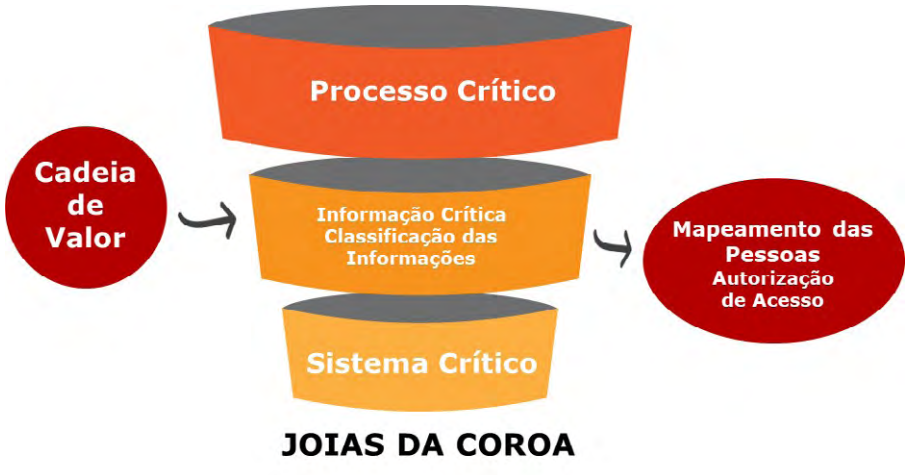
Vejam que temos que avaliar a pessoa e não o cargo, pois cada um possui características e atitudes diferentes. Por esta razão é primordial sabermos as pessoas na organização que manipulam as informações e dados sensíveis e estratégicos.

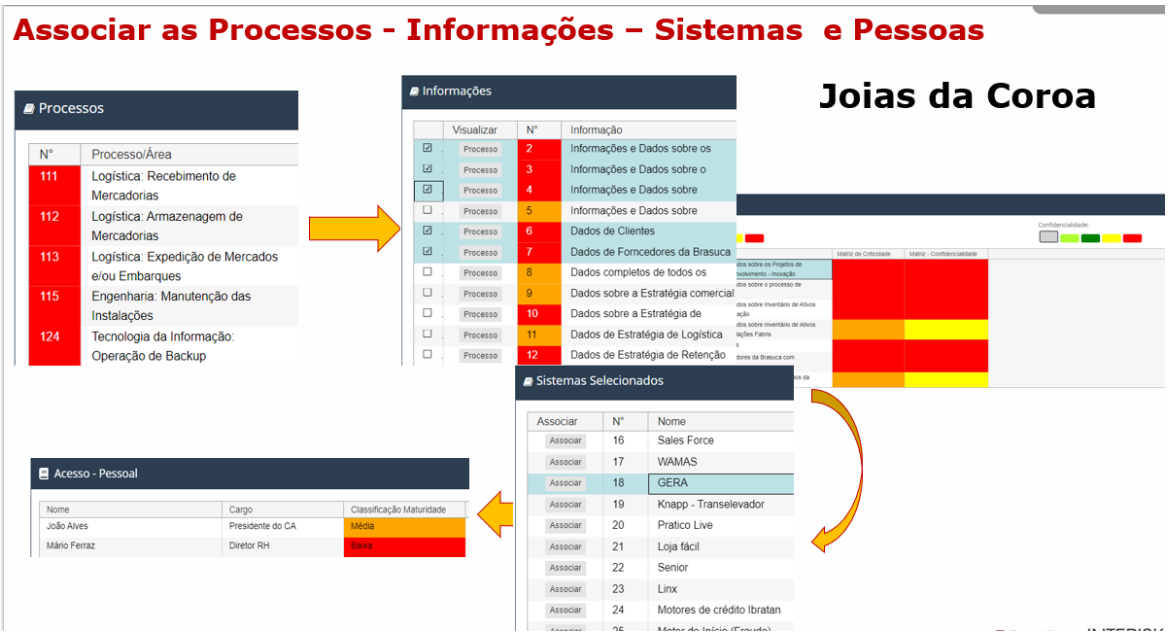
Com estes quatro passos estabelecidos, aí podemos identificar os riscos possíveis e a gestão dos ativas primordiais para a empresa. Vejam que as empresas ficam míopes em relação a estes quesitos. Se preocupam em colocar muita tecnologia e esquecem o processo estruturado de Data Loss Prevention – DLP.

O que as empresas devem entender é o que define uma Maturidade em Segurança da Informação e Cibernética é o foco nos objetivos e a interconectividade com a estratégia de negócios.

Caso não ocorra esta conexão as empresas estarão enxugando gelo, ao implantarem uma série de sistemas sem saberem suas reais fragilidades. Pergunta que não pode calar: por que os ataques cibernéticos estão em um nível exponencial, se as empresas investem milhões em sistemas? Será que estão sendo assertivas.

Nós da Brasiliano INTERISK elaboramos projetos de Data Loss Prevention - DLP no nosso sistema INTERISK, de forma centralizada, visando obter maior eficácia e controle.





Um processo estruturado de DLP coloca a empresa em grande vantagem competitiva, neste mundo BANI!

O Software INTERISK te ajuda a enxergar com antecipação suas vulnerabilidades, evitando desta forma a materialização de Vazamento de Dados.

Para saber mais sobre esses processos e como as nossas ferramentas trabalham entre em contato com um de nossos especialistas.

AMEAÇAS CIBERNÉTICAS EM CRESCIMENTO EXPONENCIAL

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CEGRC, CIEAC,
CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE e MBS.
Doutor em Ciência e Engenharia da Informação e Inteligência Estratégica pela Universit
Paris – Est (Marne La Vallée, Paris, França); presidente da Brasiliano INTERISK

Cada vez mais as organizações dependem de aplicações para estreitar relacionamentos com seus clientes e ainda fornecer seus serviços, o que faz com que enormes volumes de dados pessoais de usuários sejam armazenados. Com isso, as empresas enfrentam maior vulnerabilidade a ameaças cibernéticas e ocorrências de segurança. O desafio torna-se ainda mais sério à medida que é necessário dar suporte extra aos funcionários que trabalham em casa, utilizando notebooks e dispositivos conectados à internet pública.

Tudo isso evidencia as limitações nas práticas de monitoramento contínuo das redes empresariais, expandindo de forma geométrica o perímetro de segurança da TI. Com essa expansão, novas fragilidades e vulnerabilidades aparecem e isso exige da equipe de segurança cibernética ações e estratégicas mais abrangentes e eficazes, visando proporcionar maior nível de segurança.

Abrir mão de processos e soluções certas implantadas para salvaguardar dados armazenados não só coloca a reputação da marca e a confiança do consumidor em risco, como também custa milhões de reais as companhias, caso haja vazamento dos dados. Agora, que as aplicações rodam em qualquer lugar - desde on-premise até microsserviços nativos em múltiplas nuvens –, o novo contexto somado à inovação acelerada faz com que a necessidade de segurança direcionada seja primordial.

Essa mudança fundamental permitirá que os profissionais de segurança cibernética identifiquem vulnerabilidades dentro das aplicações durante a produção e relacionem

as vulnerabilidades e brechas com o impacto comercial, reunindo as equipes de Aplicações e de Segurança para facilitar a rápida remediação.

Ou seja, é essencial o trabalho integrado entre as áreas comerciais, operacionais e de segurança cibernética. No Brasil, poucas empresas possuem essa maturidade. O normal é ver os produtos serem lançados pelas áreas comerciais para só depois consultarem a opinião da equipe de segurança cibernética. Cria-se desde o início uma percepção que os profissionais do setor querem travar o produto, processo e o aplicativo. Porém, quando o item já está no mercado, as fragilidades são materializadas, gerando prejuízos desnecessários.

O grande diferencial nas empresas é oferecer aos times de segurança cibernética aplicativos e sistemas de segurança com maior inteligência e não mais sacrificando a segurança em prol da velocidade. Os sistemas mais modernos do segmento devem possuir a capacidade de relacionar desempenho empresarial com insights de segurança, gerando fricção zero.

É assim que as empresas protegerão suas marcas contra lentidões e exploits, que é uma sequência de comandos, dados ou uma parte do software elaborado por hackers que conseguem tirar proveito de falhas ou vulnerabilidade.

O objetivo desses criminosos é causar um comportamento acidental ou imprevisto na execução de um software ou hardware. O fato acontece tanto em computadores quanto em outros aparelhos eletrônicos. Para fins maléficos, um exploit pode dar a um hacker o controle de um sistema de computador, permitindo a execução de determinados processos por meio de acesso não autorizado a sistemas ou ainda realizar um ataque de negação de serviço.

Diferente de outros meios de disseminação de vírus e ataques cibernéticos, um exploit não precisa que o usuário clique num determinado link ou faça o download para a execução de algum arquivo. Por isso, os exploits são armas perigosas nas mãos dos hackers. Com a evolução dos computadores e dos sistemas de proteção, os hackers que utilizam exploits de maneira ilegal também desenvolveram novos métodos e diferentes ferramentas, tornando os processos que antes eram considerados seguros em obsoletos.

Em informática, exploits e vulnerabilidades possuem exatamente o mesmo significado que no mundo real. Porém, há dificuldades na definição de como uma vulnerabilidade específica aparece e o que os ladrões virtuais podem fazer para explorá-la. Muitas vezes elas são provenientes de erros na etapa de desenvolvimento de um produto.

Uma aplicação lenta ou com subdesempenho pode impactar significativamente a experiência do cliente, mas quando a segurança de uma aplicação é violada e explorada, pode haver consequências graves para o usuário final. Portanto, as empresas não podem simplesmente se darem o luxo de ignorar esse risco.

CONHEÇA AS CARACTERÍSTICAS DAS APLICAÇÕES EFICAZES E VELOZES:

- Proteção automática durante a execução: visibilidade do comportamento real de uma aplicação para facilmente detectar ataques, identificar discrepâncias e bloquear ataques automaticamente;
- Gestão simplificada de vulnerabilidades: acesso no nível do código para detecção de dependência e vulnerabilidades de segurança da produção no nível de configuração;
- Insights de segurança fundamentados pelo impacto nos negócios: informações detalhadas de segurança correlacionadas com a topologia das aplicações a fim de avaliar a relevância comercial de ocorrências de segurança e ajudar as equipes a focar as ocorrências mais importantes;
- Colaboração entre as equipes de Aplicações e de Segurança Cibernética: contexto compartilhado entre as equipes de Aplicações e de Segurança Cibernética para haver cooperação máxima, melhorando a visão de segurança. Esta parceria resultará em práticas digitais saudáveis e com uma visão de antecipação.

Concluo esse artigo afirmando aos nossos leitores que a postura de cooperação necessita de uma mudança cultural e, principalmente, da sensibilização da alta direção em relação aos riscos de ataques cibernéticos. Cabe a diretoria das empresas perguntar: se formos atacados, quando conseguimos mitigar os respectivos impactos?

Será que, nós gestores de riscos, conseguiremos atingir corações e mentes da alta gestão? Este é o nosso desafio, com um horizonte temporal pequeno, em termos de cenários: o próximo ano! Por isso, desejo sorte e sucesso nesta empreitada, pois o trabalho é e será hercúleo!

O NEGACIONISMO DA ALTA GESTÃO EM RELAÇÃO AOS RISCOS CIBERNÉTICOS FAZ COM QUE OS HACKERS SEJAM MAIS ESTRUTURADOS. POR QUÊ?

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CEGRC, CIEAC, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE e MBS.
Doutor em Ciência e Engenharia da Informação e Inteligência Estratégica pela Universit Paris – Est (Marne La Vallée, Paris, França); presidente da Brasiliano INTERISK

O risco de ataques cibernéticos é um grande rinoceronte cinza – grey rhino. Aquele animal enorme, pesado, que quando se locomove resulta num movimento massivo que destrói tudo ao redor. Hoje, qualquer tipo de organização pode virar alvo de ataques cibernéticos. Os hackers estão cada dia mais estruturados e ousados. Eles contam com um planejamento primoroso pensado de acordo com sua relação custo x benefício. Por essa razão, foi que a Colonial Pipeline nos Estados Unidos pagou o resgate exigido pelos criminosos.

Os ataques cibernéticos ocorridos nos EUA com a Colonial Pipeline, que impactou 17 estados americanos na distribuição de combustível e também a invasão nos sistemas da empresa brasileira JBS só reforçam o negacionismo dos executivos C-Level em relação aos riscos cibernéticos. Na JBS, as operações foram paralisadas totalmente, obrigando os funcionários a cortarem carnes, afiarem facas e até empacotarem seus produtos manualmente. Tudo isso abalou os negócios da organização em âmbito mundial, influenciando operações nos Estados Unidos, Canadá e Austrália.

Ao que tudo indica, os executivos das empresas ainda não possuem uma visão de antecipação e adaptação, mas é isso que o mundo pandêmico do século XXI exige (leia o artigo no qual explico o Mundo BANI. “Empresas brasileiras são alvos fáceis de hackers por falhas de segurança cibernética”, edição 154, revista Gestão de Riscos/ março 2021).

Existe a necessidade das empresas serem antifrágeis. Tal conceito está no livro de Nassim Nicholas Taleb, "Antifrágil: Coisas que se Beneficiam com o Caos". A obra é de 2012, porém o tema não poderia ser mais atual. Como também podemos ver no livro de 2008, "A Lógica do Cisne Negro", no qual o autor enumera quatro grandes erros que os executivos cometem na tentativa de racionalizar a não materialização de riscos:

1. Achar que, ao prever eventos extremos, será possível administrar o risco;
2. Acreditar que estudar o passado vai ajudar a controlar o risco. Ou seja, só olham o espelho retrovisor;
3. Pensar que o risco pode ser medido pelo desvio-padrão, apenas por métricas matemáticas. Cenários projetivos não funcionam;
4. Não entendem que a equivalência matemática não significa equivalência psicológica. Nunca levam em consideração o fator humano.

Na verdade, o risco de ataques cibernéticos é um grande rinoceronte cinza – grey rhino. Aquele animal enorme, pesado, que quando se locomove resulta num movimento massivo que destrói tudo ao redor. Hoje, qualquer tipo de organização pode virar alvo de ataques cibernéticos. Os hackers estão cada dia mais estruturados e ousados, tornaram-se criminosos profissionais, pois contam com um planejamento primoroso pensado de acordo com sua relação custo x benefício. Por esta razão, foi que a Colonial Pipeline pagou o resgate exigido.

Agora, vamos analisar. Por que há esse negacionismo? O Global Risk Report de 2007 publicou uma pesquisa entre a alta gestão de empresas e governantes. O objetivo do trabalho era entender as razões pelas quais pessoas tão qualificadas deixavam os grey rhino se deslocarem. Na pesquisa, foram identificadas que as atitudes de negação e minimização da realidade são as causas da ineficácia desse grupo avaliado. Ficou comprovado a dificuldade para lidar com os diversos tipos de riscos. Entre os motivos estão:

- Conotação negativa da palavra riscos;
- Levar em conta apenas o lado positivo;
- O risco é percebido como afetando principalmente terceiros;
- Gestão de riscos é burocracia;
- Gestão é atendimento a compliance/legislação.
- Jargão técnico excessivo. O usuário não entende.

A empresa do Sophos Rapid Response criou uma lista com os principais mitos ou percepções erradas sobre segurança cibernética mais vistos nos últimos 12 meses. O

trabalho foi feito com base na experiência e observações dos responsáveis da linha de frente no combate aos ataques cibernéticos. Veja os resultados:

Mito 1: "não somos alvo; somos muito pequenos e/ou não temos ativos de valor para um cibercriminoso".

Muitas vítimas de ataques cibernéticos presumem que são muito pequenas ou acreditam estar num setor sem interesse ou sem ativo lucrativo para atrair um cibercriminoso. A verdade é que isso não importa. Se você tem poder de processamento e presença digital, você é um alvo. Apesar das manchetes da mídia, a maioria dos ataques não é perpetrada por atacantes avançados de estados-nação. Eles são lançados por oportunistas em busca de uma presa fácil e de resultados mais fáceis, como organizações com brechas de segurança, erros ou configurações incorretas que os cibercriminosos podem explorar facilmente.

Se a organização acredita que não é um alvo, provavelmente não está procurando ativamente por atividades suspeitas em sua rede. Por esta razão, são pegos sempre de surpresa.

Mito 2: não precisamos de tecnologias de segurança avançadas instaladas em todos os lugares.

Algumas equipes de TI ainda acreditam que o software de segurança de endpoint é suficiente para barrar todas as ameaças ou pensam que não precisam de segurança para os seus servidores. Os invasores tiram total proveito dessas suposições já que quaisquer erros na configuração, patching ou proteção tornam os servidores um alvo primário e não mais secundário, como poderia ser o caso no passado.

A lista de técnicas de ataque que tentam contornar ou desabilitar o software de endpoint e evitar a detecção pelas equipes de segurança de TI, aumenta a cada dia. Os exemplos incluem ataques operados por humanos que exploram a engenharia social e vários pontos de vulnerabilidade para conseguir entrar, utilizando por exemplo código malicioso fortemente compactado e ofuscado injetado diretamente na memória. Eles também fazem uso de ataques de malware sem arquivo, como carregamento reflexivo de DLL (Dynamic Link Library) e aproveitam para efetuar o delito por meio de agentes legítimos de acesso remoto, como Cobalt Strike, juntamente com ferramentas e técnicas de administração de TI do dia a dia. Assim, as tecnologias antivírus básicas terão dificuldade em detectar e bloquear essa atividade.

Da mesma forma, a suposição de que terminais protegidos podem

impedir que invasores cheguem aos servidores desprotegidos é um erro. De acordo com os incidentes que o Sophos Rapid Response investigou, os servidores são agora o alvo de muitos ataques e os invasores podem encontrar facilmente uma rota direta usando credenciais de acesso roubadas.

A maioria dos invasores também conhece uma máquina Linux e costuma invadir e instalar backdoors para usá-los como refúgios seguros, mantendo acesso à rede de um alvo.

Se a organização depende apenas de segurança básica, sem ferramentas mais avançadas e integradas, como detecção comportamental baseada em IA e um centro de operações de segurança 24 horas por dia, 7 dias por semana, os invasores provavelmente encontrarão um caminho para além das defesas.

Por último, mas não menos importante, é sempre bom lembrar que, embora a prevenção seja ideal, a detecção é uma obrigação.

Mito 3: temos políticas de segurança robustas em vigor.

Ter políticas de segurança para aplicativos e usuários é fundamental. No entanto, eles precisam ser verificados e atualizados constantemente à medida que novos recursos e funcionalidades são adicionados aos dispositivos conectados à rede. Por isso, é importante verificar e testar as políticas, usando técnicas como teste de penetração, exercícios de mesa e testes de planos de recuperação de desastres.

Isto não ocorre nas empresas, pois elas pensam que é um custo realizar simulações e testes.

Mito 4: os servidores Remote Desktop Protocol (RDP) podem ser protegidos contra invasores alterando as portas em que estão e introduzindo a autenticação multifator (MFA).

A porta padrão usada para serviços RDP é 3389. Portanto, a maioria dos invasores varrerá essa porta para encontrar servidores de acesso remoto abertos. No entanto, a varredura identifica todos os serviços abertos, independente da porta em que estejam. Por isso, alterar as portas oferece pouca ou nenhuma proteção por si só.

Além disso, embora a introdução da autenticação multifator seja importante, ela não aumenta a segurança, a menos que a política seja aplicada a todos os funcionários e dispositivos. A atividade RDP deve ocorrer dentro dos limites de proteção de uma rede

privada virtual (VPN), mas mesmo isso não protege totalmente uma organização se os invasores já tiverem um ponto de apoio numa rede. Idealmente, a menos que seu uso seja essencial, a segurança de TI deve limitar ou desabilitar o uso de RDP interna e externamente.

Mito 5: bloquear endereços IP de regiões de alto risco, como Rússia, China e Coreia do Norte, garantem proteção contra ataques dessas regiões.

Bloquear IPs de regiões específicas provavelmente não causará nenhum dano, mas pode dar uma falsa sensação de segurança, se você confiar apenas nisso para proteção. Os cibercriminosos hospedam sua infraestrutura maliciosa em diversos países, com hotspots incluindo os EUA, Holanda e o resto da Europa.

Mito 6: nossos backups fornecem imunidade contra o impacto do ransomware.

Manter backups de documentos atualizados é essencial para os negócios. No entanto, se os backups estiverem conectados à rede, eles estarão ao alcance de invasores e vulneráveis a serem criptografados, excluídos ou desativados num ataque de ransomware.

É importante notar que limitar o número de pessoas com acesso aos backups pode não aumentar significativamente a segurança, pois os invasores terão passado algum tempo na rede procurando essas pessoas e as credenciais de acesso.

Da mesma forma, o armazenamento de backups na nuvem também precisa ser feito com cuidado. Um incidente investigado pelo Sophos mostrou que os invasores enviaram um e-mail ao provedor de serviços em nuvem de uma conta de administrador de TI hackeada e pediram que excluísse todos os backups. O provedor cumpriu.

A fórmula padrão para backups seguros que podem ser usados para restaurar dados e sistemas após um ataque de ransomware é 3: 2: 1: — três cópias de tudo, usando dois sistemas diferentes, um dos quais está offline.

Uma nota final para cautela: ter backups offline em vigor não protege suas informações de ataques de ransomware baseados em extorsão nos quais os criminosos roubam e ameaçam publicar seus dados em vez de criptografá-los.

Mito 7: nossos funcionários entendem sobre segurança.

De acordo com o State of Ransomware 2021, 22% das organizações acreditam que serão atingidas por ransomware nos próximos 12 meses por ser difícil impedir que os usuários finais estejam comprometidos com a segurança.

Táticas de engenharia social, como e-mails de phishing se tornaram difíceis de detectar. As mensagens costumam ser feitas à mão, escritas com precisão, persuasivas e cuidadosamente direcionadas. Os funcionários precisam saber como identificar mensagens suspeitas e o que fazer ao recebê-las. Quem eles notificam para que outros funcionários fiquem em alerta? Este é um dos grandes fatores de risco: o fator humano, sendo o elo mais forte e fraco da corrente chamada segurança cibernética.

Mito 8: equipes de resposta a incidentes podem recuperar dados após um ataque de ransomware.

Isto é bastante improvável. Hoje, os cibercriminosos cometem muito menos erros e o processo de criptografia melhorou, portanto, depender da reação para encontrar uma brecha que possa desfazer o dano é extremamente raro. Backups automáticos como cópias de sombra de volume do Windows também são excluídos pela maioria dos ransomwares modernos, além de sobrescrever os dados originais armazenados no disco, tornando a recuperação impossível, exceto com o pagamento do resgate.

Mito 9: pagar o resgate recupera os dados após um ataque de ransomware

De acordo com a pesquisa State of Ransomware 2021, uma organização que paga o resgate recupera em média cerca de dois terços (65%) de seus dados. Apenas 8% recuperaram todos os seus dados e 29% menos da metade. Pagar o resgate — mesmo quando parece a opção mais fácil e/ou está coberto pela sua apólice de seguro cibernético — não é, portanto, uma solução simples para ter de volta todos os dados.

Além disso, restaurar dados é apenas parte do processo de recuperação — na maioria dos casos, o ransomware desativa completamente os computadores, o software e os sistemas precisam ser reconstruídos do zero antes que os dados possam ser restaurados. A pesquisa de 2021 descobriu que os custos de recuperação são, em média, dez vezes o tamanho da demanda de resgate.

Mito 10: o lançamento de ransomware é todo o ataque, se sobrevivermos, estaremos bem.

Infelizmente, raramente é esse o caso. O ransomware é apenas o ponto em que os invasores querem que você perceba que eles estão lá e o que fizeram.

É provável que os adversários estejam em sua rede por dias, senão semanas, antes de liberar o ransomware, explorando, desativando ou excluindo backups, encontrando as máquinas com informações ou aplicativos de alto valor para criptografar, removendo informações e instalando cargas úteis adicionais, como backdoors. Manter uma presença nas redes da vítima permite que os invasores lancem um segundo ataque, se quiserem.

Esses 10 mitos fazem com que os ataques cibernéticos cresçam exponencialmente. Por esse motivo, o governo americano publicou no dia 12 de maio de 2021, uma portaria governamental a fim de fazer evoluir a segurança cibernética americana. A portaria é bastante ambiciosa, abrangente e visa, com base nos eventos recentes, minimizar a recorrência dos ataques e seus respectivos impactos.

Conheça as sete iniciativas definidas para alcançar uma maturidade considerada alta para o governo e setor privado. São elas:

1) Remoção de barreiras para o compartilhamento de informações sobre ameaças entre o governo e o setor privado. Objetiva garantir que provedores de serviços de TI compartilhem informações com o governo com obrigatoriedade para as informações relativas às violações.

2) Modernização e implementação de padrões de segurança cibernética “mais fortes” no governo federal. Proteção dos serviços em nuvem e orientação à arquitetura de confiança zero (zero-trust), com implantação de múltiplo fator de autenticação e criptografia.

3) Melhoria da segurança na cadeia de suprimentos de software. Provavelmente impactada pelo evento da SolarWinds, a ordem endereça a preocupação com a definição de padrões básicos de segurança para o desenvolvimento de software que seja vendido ao governo, demandando que os desenvolvedores avancem em aspectos de segurança. A exemplo dos selos de consumo de energia para eletrodomésticos, será desenvolvido um selo de qualidade para que o governo e público em geral possa identificar quais softwares foram desenvolvidos dentro dos padrões de segurança esperados.

4) Estabelecimento de um Conselho de Revisão de Segurança Cibernética. O conselho será composto por membros do governo e setor privado, o qual poderá ser acionado após um incidente cibernético significativo

para analisar o evento e emitir recomendações concretas para evolução da segurança cibernética. De forma análoga esse processo é realizado no âmbito da aviação para que acidentes não se repitam.

5) Criação de um manual padrão para resposta a incidentes de segurança cibernéticos. A portaria cria um manual padronizado para a resposta aos incidentes cibernéticos por departamentos e agências federais. O manual visa garantir que todas as agências federais americanas estejam preparadas para tomar medidas uniformes para identificar e mitigar uma ameaça, bem como responder. Esse manual servirá de modelo para o setor privado.

6) Melhoria da detecção de incidentes de segurança cibernética em redes do governo federal. Objetiva melhorar a capacidade de detecção de atividades cibernéticas nas redes federais, permitindo um sistema de detecção e resposta em toda administração e o compartilhamento de informações entre o próprio governo. Dessa forma, a gestão pública deverá liderar a evolução da segurança cibernética.

7) Melhoria da capacidade de investigação e correção. A ordem cria requisitos de registros de eventos de segurança cibernética para departamentos e agências federais. Nesse item, há o reconhecimento de que a deficiência em registros (logs) prejudica a capacidade das organizações na detecção, mitigação e compreensão das investidas criminosas, sejam as ocorridas ou as que ainda estão em curso.

Com essa portaria, fica claro que o tema segurança cibernética está sendo levado cada vez mais com seriedade e que o governo americano reconhece a necessidade de evolução tanto em agências governamentais quanto no setor privado. A portaria exigirá que o estado que dê o exemplo e evolua suas capacidades de segurança, que por manobra resultará na evolução do setor privado.

Não é uma tarefa fácil, mesmo para o governo americano, pois a portaria prevê diversos prazos para implementação das ações e objetivos. Como há grande desequilíbrio na maturidade, no governo e no setor privado, pode haver reflexos em descumprimento de boa parte dos órgãos e instituições.

No entanto, é uma iniciativa extremamente positiva, pois o governo deu um primeiro passo, no sentido de alavancar a segurança cibernética. Seria muito positivo se o governo brasileiro também desse o exemplo e objetivasse também a evolução de sua segurança cibernética.

Espero que o Brasil e suas empresas estatais e privadas cresçam em seu nível de maturidade. Noto no mercado grandes falhas e uma visão da alta gestão ainda bastante incipiente. Por isso, vale lembrar a máxima de Frederico, o Grande, que disse: “Perdoável ser derrotado, mas nunca surpreendido”.

POR QUE AS INFRAESTRUTURAS CRÍTICAS NO MUNDO CONTINUAM SENDO ALVO DE ATAQUES CIBERNÉTICOS?

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CEGRC, CIEAC, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE e MBS.

Doutor em Ciência e Engenharia da Informação e Inteligência Estratégica pela Universit Paris – Est (Marne La Vallée, Paris, França); presidente da Brasiliano INTERISK

Há necessidade urgente de haver uma mudança radical de mentalidade (mindset) por parte dos gestores de segurança cibernética de infraestruturas críticas (IC).

Quando falamos em "mindset", significa que falamos sobre uma nova configuração da mente, conceito inovador que busca entender a predisposição psicológica de uma pessoa que prioriza determinados pensamentos e padrões de comportamento para, então, propor e desenvolver uma nova abordagem. É imprescíndivel que os gestores de segurança cibernética elaborem condutas diferentes para sensibilizar a alta gestão das infraestruturas críticas, que não acredita que ser alvo, negam a realidade, não conhecem o perfil de seu negócio e respectiva atratividade.

Hoje no século XXI, as IC são alvos declarados. Os ataques cibernéticos em IC possuem objetivos diferentes: vão desde questões político-sociais, fins lucrativos, geopolíticas ou até mesmo ciberespionagem de nação para nação. Os principais alvos dos cibercriminosos e hacktivistas hoje são as infraestruturas de energia. A eletricidade é considerada mais vulnerável. Depois vem petróleo, gás, transporte, serviços públicos, telecomunicações e setores críticos de manufatura. Além disso, os riscos de ataque com ransomware afetam a saúde pública e visam as cadeias de suprimentos médicos. O trabalho remoto que foi ampliado em virtude da pandemia Covid-19 também virou uma oportunidade para ataques cibernéticos.

O conceito de infraestrutura crítica inclui ativos, sistemas, instalações, redes e outros elementos dos quais um país depende para manter a segurança nacional, a vitalidade

econômica e a saúde pública. São inúmeros os setores considerados como críticos, que possuem dependência da internet para sua operação, gestão e automação. Então por que são negligenciados? Na minha opinião, são dois motivos:

- O primeiro tem um viés psicológico de negar que a infraestrutura não é alvo. A alta gestão formada por diferentes perfis de executivos não acreditam nesta possibilidade;

- O segundo é a falta de conhecimento. Existe uma certa ignorância no assunto, pois muitos pensam que o pessoal de TI resolve totalmente o problema. Focam apenas na tecnologia e não no negócio. Quando falo isso, quero dizer que o gestor de segurança cibernética tem que saber, antes de pensar em tecnologia pura, quais são: os processos críticos da IC, as informações atrativas e estratégicas e quais os sistemas digitais que suportam os processos críticos e as informações. Uma quarta questão também estratégica e primordial é conhecer o nível de maturidade das pessoas que possuem autorização para acessar e usar as informações.

Não podemos esquecer que quase 90% dos ataques cibernéticos no mundo tiveram portas de acesso abertas por meio de e-mails maliciosos, denominados de Phishing. Diante dessas informações, o gestor deve começar a pensar nas portas abertas dos processos e caminhos críticos.

Denomino essas quatro informações como sendo as “Joias da Coroa”. Ou seja, sem ter esse conhecimento não tem como começar em pensar em segurança cibernética. E os hackers sabem disso, por isso planejam os ataques estruturados com base neste “gap”. No nosso software INTERISK, há uma disciplina específica de Cibernética, que mostra como as Joias da Coroa estão na 1a Fase do Framework de Gestão de Riscos Cibernéticos.

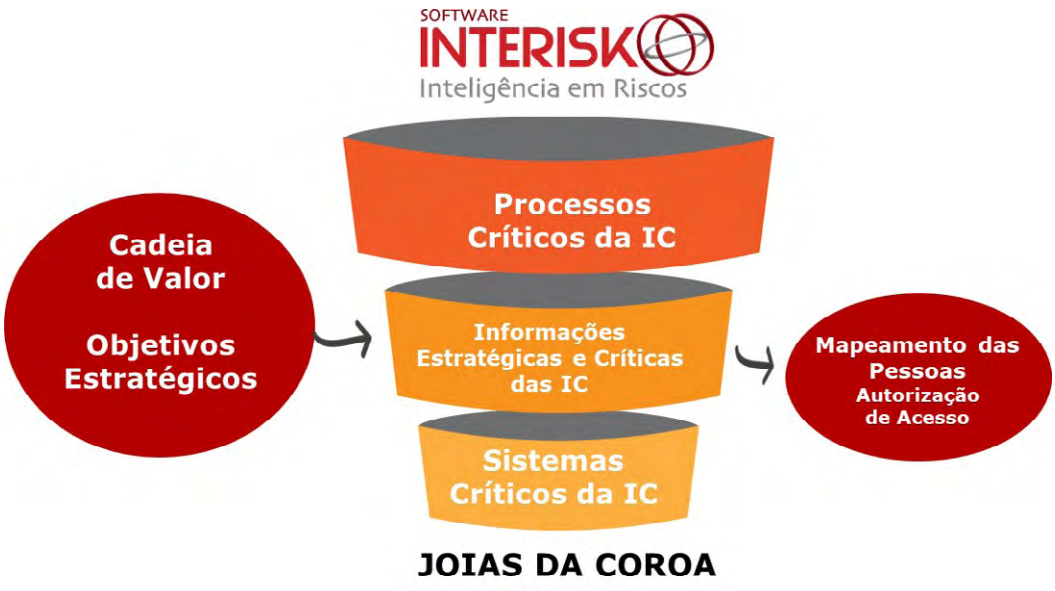


Figura 1: Joias da Coroa. Fonte: Brasiliano INTERISK

Por esta razão é que as infraestruturas críticas estão em risco, pois se tornaram os principais alvos pela simples razão de demonstrarem inúmeras fragilidades na grande superfície de ataque. Os agressores consideram alvos fáceis, além de oferecem visibilidade para que os hackers ganhem reputação. É assim que eles conseguem altos valores em resgate e criam distrações, criando também alvos em potencial para guerras cibernéticas ou ataques contra países. Ou seja, a atratividade é muito alta e aí a propensão de ataque cresce em escala exponencial.

Outro grande erro das infraestruturas críticas é não elaborarem Cenários de Ataques e como que eles podem ocorrer. Para isso, devem possuir as seguintes informações:

1. O negócio da infraestrutura crítica;
2. Os impactos para o país, estado e cidade que a IC presta serviço, consequência do impacto na operação, impacto financeiro, legal e imagem;
3. Fragilidades existentes, condição de segurança na Joias da Coroa, levando em consideração pessoas, controles lógicos, controles físicos e processos;
4. Perfis de agressores, dos hackers, suas características e modus operandi;
5. Pensar como um agressor, tendo em vista as informações acima, como que minha infraestrutura crítica pode ser invadida.

Podemos ter uma visão holística de possíveis ataques cibernéticos por meio do diagrama de causa e efeito abaixo:

Figura 2: Diagrama de Causa e Efeito de Cenários de Ataques Cibernéticos.
Fonte: Brasiliano INTERISK

Com base na montagem de Ameaças Inteligentes, como o diagrama acima, as infraestruturas críticas podem possuir visão de antecipação. Exemplo: saberem que atualmente os ataques são automatizados e muito rápidos. O perfil dos hackers hoje não são mais pessoas solitárias hackeando para se divertirem, mas sim estruturas empresariais nas sombras ou grupos apoiados por nações que têm muita tecnologia

e apoio financeiro e lançam ataques sofisticados com inteligência artificial para encontrarem as brechas. Brechas são as portas de acesso que podem ser até de um dispositivo de segurança física, do tipo um CFTV ligado na rede.

Com os cenários cada vez mais sofisticados, a segurança cibernética deve ter ferramentas de nível igual e/ou superior dos seus agressores, do tipo automação que incluam inteligência artificial, machine learning e redes de autocura (sistemas que se protegem). Isto é estar no século XXI!

Isolar infraestruturas críticas, isto é, removê-las de redes e conexões, não resolve mais o problema porque a cadeia de fornecimento do software dessa infraestrutura tem que passar, de qualquer maneira, por redes que podem estar comprometidas por ataques.

As causas mais comuns exploradas pelos criminosos cibernéticos são os sensores industriais de todos os tipos, firewalls antigos e sistemas de segurança mal configurados, links a banco de dados, acesso telefônico ou conexões de gerenciamento de rede secundária e VPNs, citando apenas algumas. Por outro lado, os sistemas de controle industrial são difíceis de proteger porque alguns são muitos antigos, mas ainda funcionam, e não levam a segurança em consideração. O que é o mais comum. A Tecnologia de Automação – TA nas infraestruturas críticas focam na disponibilidade, o que é correto desde que tenham confidencialidade/segurança.

Cito como exemplo o ataque em 7 de maio, nos Estados Unidos na maior empresa de gasoduto, a Colonial Pipeline, por meio de ransomware, impactando 17 estados americanos, em um trecho de aproximadamente 8.850 quilômetros, abrangendo do Texas até Nova York. Vejam que estamos falando dos Estados Unidos, que em função desse ataque desabasteceu 17 estados. Impacto massivo. A empresa confirmou o ataque cibernético no dia seguinte e alegou que para conter a ameaça eles tiveram que desconectar alguns computadores. Está aí a fragilidade exposta!

Mudar a mentalidade é essencial

No contexto atual, os criminosos cibernéticos estão ajustando suas táticas e a inovação digital, consequentemente criando mais riscos. A adição da alta conectividade, tornado a superfície de proteção extremamente grande e abrangente, fragilizou a segurança cibernética. Hoje o perímetro das redes está em toda parte e, com a transição para a nuvem, estão vindo novas vulnerabilidades, assim como com a Internet das Coisas (IoT), que expandiu os pontos de acesso e está permitindo que os invasores encontrem sistemas e serviços abertos por meio de câmeras, roteadores e servidores, entre outros dispositivos.

Muitos tomadores de decisões corporativas e governamentais acreditam que, se estiverem na nuvem, estarão protegidos automaticamente. Doce ilusão! A realidade é que deve haver segurança cibernética de ponta a ponta: desde o dispositivo do funcionário e da VPN até a instância da nuvem, envolvendo toda a infraestrutura híbrida. Além disso, as organizações devem ter visibilidade centralizada de tudo que

acessa e passa por sua rede, fácil gerenciamento e automação.

A mudança do “mindset” é fundamental. A implementação de um esquema de segurança cibernética de ponta a ponta deve ser a prioritária. Para isso, os gestores de segurança cibernética devem ser pontuais e saberem onde investir. Portanto, eles devem conhecer suas fragilidades do tipo gráfico radar.

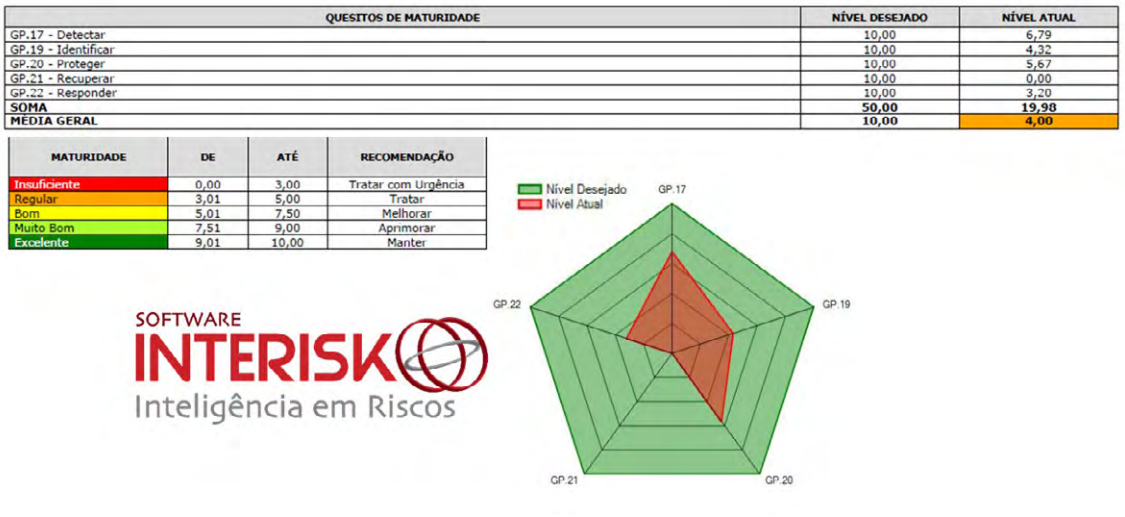


Figura 3: Gráfico Tipo Radar – Nível de Maturidade – Fornece uma visão pontual onde encontra as fragilidades. Fonte: Brasiliano INTERISK

Uma pesquisa recente realizada pela Fortinet indica que as organizações estão se movendo na direção errada em termos de resultados. Nove em cada dez empresas experimentaram pelo menos uma intrusão de OT (tecnologia operacional), em 2020, foram 19% a mais do que em 2019. E a proporção de organizações que experimentaram três ou mais intrusões aumentou de 47% para 65% durante o mesmo período.

Sabemos que a segurança cibernética na Tecnologia de Automação – TA ainda caminha a passos lentos e o desconhecimento é brutal. Os criminosos cibernéticos aproveitam essa fragilidade e realizam suas invasões, afetando a eficiência operacional, a receita e até a segurança física das empresas. Com o aumento da conectividade dos sistemas de TA com sistemas de TI e a Internet, as redes de negócios estão se tornando mais complexas, dificultando a proteção abrangente. A pesquisa mostrou o que descrevemos neste artigo, que uma porcentagem significativa das infraestruturas críticas não possui uma segurança cibernética com elementos básicos em seus ambientes de TA. Este é um dos grandes problemas a ser resolvido. Sensibilizar a alta gestão de TA no quesito cibernético. A segurança cibernética não deve ser um plano futuro, mas sim ação imediata, consistente e eficaz. Basta mudarmos o “Mindset”! Conseguiremos?

LIDERANÇA HUMANIZADA NA SEGURANÇA EMPRESARIAL

Anderson Moura, MBS, CPSI, CIGR, CIEIE, EAR, MBA
Gestor de Segurança Especialista no Setor Elétrico

É indiscutível que os gestores de segurança empresarial buscam a cada dia mais conhecimento técnico em gestão de riscos, soluções tecnológicas, métodos e ferramentas de qualidade visando melhoria contínua e medição do desempenho da sua área. Todas as disciplinas legítimas e necessárias ao profissional de segurança.

Seguindo este racional é importante citar o Professor Msc. Carlos Caruso onde na sua obra Guia do Gestor de Segurança menciona as competências do gestor de segurança empresarial: *"Todavia, o gestor de segurança, sem dúvida, tem uma função muito mais administrativa. Sendo responsável pela área é importante que tenha conhecimentos multidisciplinares para conduzir sua área com eficácia e sucesso. Além dos aspectos operacionais e das rotinas, deve ter uma visão mais ampla, que envolve administração, análise e gestão de riscos, elaboração de relatórios, planilhas, apresentações, condução de reuniões, gestão de contratos, cronogramas, planejamento estratégico, organização, orçamentos anuais, liderança e motivação de equipes, gestão de operações, ética profissional, noções de comunicação empresarial, de marketing pessoal, além de outras competências."* Em especial, observa-se duas competências citadas pelo professor Caruso: Liderança e Motivação da Equipe.

O Professor Nino Ricardo Meireles em sua obra Liderança do Gestor de Segurança conjetura sobre o papel de liderança do gestor de segurança: *"O gestor, para exercer com eficiência e eficácia as suas atividades, precisa não apenas ser um chefe, mas, sobretudo, um líder. Apesar de muitos afirmarem que não se pode formar um líder, entendemos que esta afirmação não é totalmente verdadeira, mas, sem dúvida*

alguma, o líder nato sempre sobressairá em relação ao líder formado."

Para falar da competência liderança na segurança empresarial se faz necessário pensar sobre a maneira empregada por alguns gestores pela essência. O modelo militar, de comando e controle, onde o superior dá a ordem e o subordinado simplesmente obedece não coopera para o desenvolvimento pessoal, cumprimento dos objetivos da área e, principalmente, o clima organizacional. Isso, porque exerce retração entre os membros da equipe.

Contribuindo para evolução deste pensamento é importante conjeturar sobre o pensamento do economista e ativista Paul Gerard Hawken: *"Nós lideramos sendo humanos. Nós não lideramos sendo corporativos, sendo profissionais ou sendo institucionais."*

Para evoluir neste racional, cabe-se algumas reflexões:

a. Você, profissional de segurança privada conheceu em sua trajetória quantos líderes do seguimento que se preocupavam realmente com você como pessoa?

b. Quantas vezes percebeu claramente que seu líder se colocou em seu lugar? Apresentando ali empatia.

c. Você já trabalhou com algum gestor de segurança que agia com seus subordinados como fosse uma celebridade e não o líder da área?

d. Foi liderado por pessoas inacessíveis?

Se para alguma das perguntas acima a resposta foi sim, recomendo concluir a leitura deste artigo de opinião.

Em fevereiro de 2019 percebi que o melhor estilo de liderança que eu poderia adotar seria a humanizada. Esta opção se deu simplesmente pelo fato de ter atuado muito tempo no nível operacional e saber, não somente pela teoria e sim na prática a importância de ser liderado por alguém que realmente se importa com pessoas. O gestor de segurança pode ter planejamento robusto em todos os níveis: Estratégico, Tático, Técnico e Operacional. Porém, inevitavelmente, o elo mais fraco desta corrente sempre serão as pessoas.

Para tangibilizar este pensamento, certa vez acompanhava a mobilização de implantação dos serviços de vigilância e portaria. O gerente operacional da empresa de segurança patrimonial contratada ao notar minha presença em sua sede, de forma muito gentil, veio me saudar e apresentar as atividades ali realizadas para o início da prestação de serviços. Surpreendentemente percebi que ele não cumprimentou o supervisor de segurança patrimonial, empregado da empresa dele e dedicado ao contrato por mim gerido que estava ao meu lado. A fim de corrigir este lapso, apresentei o supervisor ao gerente que simplesmente ignorou a presença do

supervisor e continuou falando somente comigo. Neste momento, automaticamente, percebi a dificuldade que teria com aquela empresa, fato que verdadeiramente ocorreu no transcorrer dos meses.

Entender que cada colaborador é único faz toda a diferença no clima organizacional e no cumprimento dos objetivos pela equipe.

Portanto, o gestor de segurança que pretende adotar o estilo Liderança Humanizada deve aprimorar as capacidades abaixo:

DESENVOLVA EMPATIA

Empatia é a capacidade do líder se colocar no lugar liderado, vivenciando seus sentimentos e necessidades. Isso, visando identificar abertamente o que o subordinado realmente necessita, de forma legítima, não somente o que ele deseja.

Deste modo, empatia é uma característica fundamental na liderança, considerando que os membros possuem personalidades muito diversificadas, com histórias de vida variadas e experiências singulares captadas ao longo das suas carreiras na segurança.

Nesse contexto é importante entender a empatia como instrumento de gestão. Porquanto, os pensamentos e atos empáticos do líder, quando vistos como uma ação cotidiana, fomentam diretamente uma relação de confiança e colaboração no time.

"Poderia haver maior milagre do que olharmos com os olhos do outro por um instante?" Henry David Thoreau (pesquisador, historiador e filósofo).

SAIBA OUVIR

Um dos piores pecados de um líder é acreditar que falar é mais importante do que ouvir.

As principais vantagens em ouvir mais e falar menos são:

- Entender as pessoas antes de começar a liderá-las;
- É a melhor maneira de aprender;
- Pode impedir que os problemas se avolumem;
- Estabelece relações de confiança;
- Alegra seus liderados pela atenção fornecida.

"Saber ouvir estabelece um vínculo de confiança, que é o fundamento de todos os relacionamentos duradouros" Brian Tracy (escritor).

MOTIVE SEU TIME

Abaixo seguem algumas formas para motivar e reter os talentos do seu time:

- Mantenha seu time envolvido e trabalhando pelos mesmos objetivos;
- Tenha um bom canal de comunicação entre você e seus colaboradores. Deve-se estar sempre acessível, já que nem sempre estará disponível;
- Seja claro e objetivo nas descrições das tarefas e o que se espera exatamente de cada membro do time;
- A confiança no time encoraja o pensamento independente, aumenta a autoconfiança e o senso de autoestima, por isso delegue;
- Faça que todos se sintam parte da empresa, encorajando-os a participar das análises para soluções de problemas;
- Impulsione o desempenho através do aprendizado;
- Proporcione um ambiente que possibilite crescimento pessoal, realização e reconhecimento.

"O homem começa a morrer na idade em que perde o entusiasmo." Honoré de Balzac (escritor).

DESENVOLVA AS PESSOAS

Além dos treinamentos e dos diálogos diários, amplamente realizados pelos gestores de segurança empresarial visando à padronização das atividades e evolução dos profissionais de segurança é de extrema importância dar Feedback de forma assertiva.

"Promover o crescimento e o desenvolvimento pessoal é o maior chamado de um líder." Dale Galloway (escritor).

No Feedback deve-se ponderar evitando os extremos (repreensões ou confetes), pois se trata de uma ferramenta para adequação de comportamentos, motivação e retenção de talentos. É a base da evolução de uma equipe para um verdadeiro time, ajudando no alinhamento dos membros no encargo de alcançar os objetivos planejados.

No processo de desenvolvimento destaca-se o Feedback corretivo. É importante que a ação de adequação seja realizada de forma imediata e pontual visando auxiliar em mudanças no desempenho. Para ter o efeito desejado essa ação exigirá do líder muito preparo e cuidado com a escolha das palavras a serem empregadas.

"A crítica é algo que você evita com facilidade; é só não falar nada, não fazer nada e não ser nada". Aristóteles (filósofo).

LIDERE POR EXEMPLO

A credibilidade de um líder começa com o sucesso pessoal e se confirma na iniciativa de ajudar os outros a alcançar sucesso também.

Neste diapasão, jamais pregue algo que você mesmo não acredite e/ou não cumpre.

É importante que todos os membros do time sintam que poderão contar com um líder sincero, seguro e bem preparado.

"O verdadeiro líder se revela antes de ser promovido, ao conquistar a confiança das pessoas". Max Gehringer (administrador de empresas e escritor).

CONSTRUA UM TIME

Acredito que a construção de um time virá naturalmente da evolução de um grupo. E o líder possui protagonismo neste processo a partir da seleção do seu grupo.

Se todos os integrantes não "tocarem a mesma música" haverá apenas um grupo e não um time.

De certo, selecione pessoas que:

- Complementem as deficiências do grupo;
- Estejam realmente interessadas em aprender;
- Possuam espírito de trabalho em grupo;
- Tenham atitudes fundamentadas nos procedimentos.

"Eu sou parte de uma equipe. Então, quando venço, não sou eu apenas quem vence. De certa forma, termino o trabalho de um grupo enorme de pessoas". Ayrton Senna (piloto).

Tendo em vista tudo o que foi mencionado, o estilo de gestão humanizada se aplica a todas as categorias profissionais, afinal todo profissional é um gestor de pessoas. Outrossim, o gestor de segurança empresarial possui oportunidade ímpar em adotar o estilo da Liderança Humanizada e transformar seu grupo em verdadeiro time. Extraindo o melhor de cada membro, alavancando o desempenho da área e melhorando o clima organizacional.

"Nada é mais conclusivo para aprovar a capacidade de liderança de um homem que as ações empreendidas, dia após dia, para liderar a si mesmo." Thomas John Watson (empresário).